LLICENCIATURA DE MATEMÀTIQUES

APUNTS

ÀLGEBRA ABSTRACTA

Jordi Quer
Departament de Matemàtica Aplicada 2

MAT
AA

UPC
FME Facultat de Matemàtiques i Estadística
UNIVERSITAT POLITÈCNICA DE CATALUNYA

APUNTS D'ÀLGEBRA ABSTRACTA

Jordi Quer

Temari

Tema I: GRUPS

1.– Grups i subgrups

Definició. Un *grup* és un conjunt on hi ha definida una operació associativa, amb element neutre, i tal que tot element té invers. Es diu *abelià* si l'operació és commutativa.

Notacions additiva i multiplicativa. Són habituals les notacions *additiva* i *multiplicativa*. En la primera, l'operació es denota $+$, el neutre 0, i l'invers de l'element a és $-a$; si n és un enter i $a \in G$, na és el resultat d'operar a n vegades. En notació multiplicativa l'operació es denota com es fa habitualment amb el producte, el neutre és 1, i l'invers de a és a^{-1}; el resultat d'operar a n vegades és a^n i valen les regles usuals d'exponenciació. Pels grups abelians es sol fer servir la notació additiva i per grups en general la multiplicativa.

Subgrups. Un *subgrup* H d'un grup G és un subconjunt que és un grup respecte l'operació de G. Això equival a dir que H és no buit i tancat respecte l'operació de G i fer l'invers. La intersecció de subgrups és clarament un subgrup. Tot grup G té almenys dos subgrups: el trivial, format només per l'element neutre (que denotarem simplement 1) i el propi G.

Si S és un subconjunt de G, el *subgrup generat* per S és la intersecció de tots els subgrups que el contenen; es denota $\langle S \rangle$ i està format per tots els productes $a_1 \cdots a_r$ d'elements que són de S o són inversos d'elements de S.

Els subgrups d'un grup formen un reticle amb la inclusió. L'ínfim d'una família de subgrups és la seva intersecció i el suprem és el subgrup generat per la seva reunió.

Un grup es diu *finitament generat* si existeix algun subconjunt finit que el genera. Es diu *cíclic* si es pot generar amb un sol element.

Ordre. L'*ordre* d'un grup és el seu cardinal i ordre d'un element és l'ordre del subgrup cíclic que genera. Si un element $a \in G$ té ordre finit, aquest ordre és l'enter més petit, $n \geqslant 1$, tal que $a^n = 1$; quan no existeix cap enter amb aquesta propietat a té ordre infinit.

Classes laterals. Sigui H un subgrup de G. Els subconjunts aH per $a \in G$ s'anomenen *classes laterals* per l'esquerra. Anàlogament, es defineixen les classes laterals per la dreta com els conjunts Ha.

Les classes laterals per l'esquerra (resp. dreta) són una partició de G; es tracta de la partició en classes d'equivalència corresponent a la relació d'equivalencia $a \sim b \Leftrightarrow a^{-1}b \in H$ (resp. $ab^{-1} \in H$). El conjunt de classes per l'esquerra es denota G/H; el de les classes per la dreta $H\backslash G$.

L'aplicació $x \mapsto ax$ és una bijecció de H en aH; en particular totes les classes laterals per l'esquerra tenen el mateix cardinal (anàlogament per la dreta). Com a consequència, en el cas dels grups finits, l'ordre d'un subgrup (i, en particular, d'un element) divideix l'ordre del grup.

S'anomena *índex* del subgrup H al grup G el cardinal del conjunt de classes per l'esquerra i es denota $[G : H] = |G/H|$. Quan G és finit aquest cardinal és el quocient $|G|/|H|$. L'índex es comporta multiplicativament: si $H \subseteq K$ són subgrups de G, aleshores

$$[G : K] = [G : H] \cdot [H : K]$$

Homomorfismes. Un *homomorfisme* (o morfisme) de grups és una aplicació $f\colon G_1 \to G_2$ compatible amb les operacions; o sigui, amb $f(ab) = f(a)f(b)$.

Si H_1 és subgrup de G_1, $f(H_1)$ ho és de G_2; si H_2 és subgrup de G_2, $f^{-1}(H_2)$ ho és de G_1. En particular el *nucli* de f és el grup $f^{-1}(1) \subseteq G_1$, que es denota $\operatorname{Ker} f$ (de l'alemany kernel). Observem també que la imatge $\operatorname{Im} f = f(G_1)$ és un subgrup de G_2.

La composició d'homomorfismes és un homomorfisme. Un *monomorfisme* (resp. *epimorfisme*, *isomorfisme*) és un homomorfisme injectiu (resp. exhaustiu, bijectiu). L'aplicació inversa d'un isomorfisme és també un isomorfisme. Un *endomorfisme* és un homomorfisme d'un grup en ell mateix, i es diu *automorfisme* si és bijectiu. Els automorfismes d'un grup G són, amb l'operació composició, un grup, que es denota $\operatorname{Aut} G$.

Un homomorfisme és injectiu si i només si el seu nucli és trivial.

Dos grups són *isomorfs* si existeix un isomorfisme de l'un a l'altre. S'escriu $G_1 \simeq G_2$ per indicar que els grups G_1 i G_2 són isomorfs. La relació "ésser isomorfs" és d'equivalència. Dos grups isomorfs són indistingibles des del punt de vista de la seva estructura.

Un *diagrama* de grups i homomorfismes és un graf (orientat) que té per vèrtexs grups i per arestes homomorfismes de grups. El diagrama es diu *commutatiu* quan sempre que hi hagi més d'un camí per anar d'un vèrtex a un altre els homomorfismes corresponents coincideixin. Una successió de grups i homomorfismes

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

s'anomena *exacta a* G_i si $\operatorname{Im} f_{i-1} = \operatorname{Ker} f_i$ i *exacta* si ho és a tots els grups. En particular, la successió

$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1$$

és exacta si i només si f és monomorfisme, g epimorfisme, i $\operatorname{Im} f = \operatorname{Ker} g$. Una successió com aquesta es diu *successió exacta curta*, i el grup G s'anomena una *extensió* del grup K pel grup H (encara que alguns autors en diuen extensió de H per K).

Subgrups normals i grup quocient. Un subgrup $H \subseteq G$ és *normal* si les classes laterals per la dreta coincideixen amb les classes laterals per l'esquerra; o sigui, si $aH = Ha$ per tot $a \in G$.

En tal cas el conjunt de classes laterals G/H hereda una estructura de grup amb l'operació de multiplicar classes $(aH)(bH) = aHbH = abH$ i s'anomena *grup quocient* de G per H.

L'aplicació $\pi\colon G \to G/H$ definida per $a \mapsto aH$ és un homomorfisme de grups anomenat *homomorfisme canònic* (o projecció canònica). Es tracta d'un epimorfisme i el seu nucli és el subgrup H.

Es comprova immediatament que els subgrups normals es caracteritzen també pel fet de ser el nucli d'algun homomorfisme.

Siguin $H \subseteq K$ subgrups d'un grup G. Si H és normal a G aleshores també ho és a K; naturalment, pot ser normal a K i no ser-ho a G. La normalitat no és transitiva: pot ser que H sigui normal a K i K ho sigui a G pero que H no ho sigui a G.

Sigui $f\colon G_1 \to G_2$ un homomorfisme. Si H_2 és un subgrup normal de G_2, $f^{-1}(H_2)$ és normal a G_1. Si H_1 és un subgrup normal de G_1, $f(H_1)$ és normal a $\operatorname{Im} f$ però no te perquè ser-ho a G_2.

La projecció canònica estableix una bijecció (de fet, un isomorfisme de reticles) entre els subgrups de G/H i els subgrups de G que contenen H; els subgrups normals a un costat es corresponen amb els subgrups normals a l'altre.

Si H és un subgrup normal de G, tenim una successió exacta curta

$$1 \longrightarrow H \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } G/H \longrightarrow 1$$

i tota successió exacta curta es correspon, essencialment, a una situació com aquesta.

Teorema d'isomorfisme. Sigui $f\colon G_1 \to G_2$ un homomorfisme. L'aplicació

$$f_*\colon G_1/\operatorname{Ker} f \to \operatorname{Im} f, \qquad a(\operatorname{Ker} f) \mapsto f(a)$$

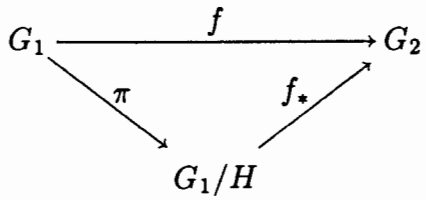
està ben definida i és un isomorfisme de grups. Aquest fet, de comprovació trivial, es coneix com el (primer) *teorema d'isomorfisme*.

L'aplicació f descompon de la manera següent

$$G_1 \xrightarrow{\ \pi\ } G_1/\operatorname{Ker} f \xrightarrow{\ f_*\ } \operatorname{Im} f \longrightarrow G_2$$

com a producte de l'aplicació canònica π (epimorfisme), l'isomorfisme f_* i el monomorfisme inclusió.

Sigui H un subgrup normal de G_1. Diem que f factoritza a través de G_1/H si existeix un homomorfisme f_* que faci commutatiu el diagrama següent:



Es comprova fàcilment que això passa si, i només si, $H \subseteq \operatorname{Ker} f$ i que, en tal cas, f_* queda determinat per $f_*(aH) = f(a)$.

Producte directe. Siguin G_1 i G_2 grups. El seu *producte directe* (extern) és el producte cartesià $G_1 \times G_2$ amb l'operació definida component a component. Anàlogament es defineix el producte directe d'un nombre finit de grups $G_1 \times \cdots \times G_k$ i, fins i tot, d'una família arbitrària. Sigui $G = G_1 \times \cdots \times G_k$. Donat $1 \leqslant i \leqslant k$, el subconjunt dels elements que tenen un 1 a totes les coordenades $j \neq i$ és un subgrup normal de G isomorf a G_i.

Conjugació. Els *conjugats* d'un element $a \in G$ són els elements de la forma xax^{-1}, per $x \in G$. La conjugació defineix una relació d'equivalència a G; les classes d'equivalència corresponents s'anomenen *classes de conjugació*.

De manera anàloga, es defineixen els conjugats d'un subconjunt $S \subseteq G$ com els subconjunts xSx^{-1}. Es tracta de subconjunts amb el mateix cardinal que S i, si H és un subgrup, els seus conjugats també ho són. La conjugació proporciona també una partició del conjunt de les parts de G i del conjunt dels subgrups de G.

Fixat un $x \in G$, la conjugació per x, $a \mapsto xax^{-1}$, és un automorfisme $\gamma_x \colon G \to G$. L'aplicació $G \to \operatorname{Aut} G$ donada per $x \mapsto \gamma_x$ és un homomorfisme de grups. La seva imatge, formada pels automorfismes que són conjugacions, s'anomena el grup dels *automorfismes interns* de G, i es denota $\operatorname{Inn} G$. El grup $\operatorname{Inn} G$ és un subgrup normal de $\operatorname{Aut} G$.

Centralitzadors i normalitzadors. Si $a \in G$, el seu *centralitzador* es defineix com $Z_G(a) = \{x \in G \mid xax^{-1} = a\}$. Es tracta del conjunt dels elements de G que commuten amb a. Si $S \subseteq G$, el seu centralitzador és $Z_G(S) = \{x \in G \mid xax^{-1} = a \ \forall a \in S\} = \bigcap_{a \in S} Z_G(a)$. Els centralitzadors són subgrups de G. El centralitzador de tot G s'anomena *centre* de G i es denota $Z(G)$; és un subgrup normal i $G/Z(G) \simeq \operatorname{Inn} G$.

Si $S \subseteq G$, el seu *normalitzador* és el conjunt $N_G(S) = \{x \in G \mid xSx^{-1} = S\}$. És també un subgrup de G. Un subgrup H és normal a $N_G(H)$. De fet, el normalitzador és el subgrup de G més gran dins el qual H és normal. En particular, H és normal a G si, i només si, $N_G(H) = G$.

2.– Exemples

- Els conjunts de nombres $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ són grups amb l'operació suma. Els conjunts $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ són grups amb el producte.
- Si R és un anell unitari, el conjunt dels elements invertibles $R^* = \{x \in R \mid \exists y \in R, xy = yx = 1\}$ amb el producte de l'anell és un grup, anomenat *grup multiplicatiu* de R. Quan R és un cos, $R^* = R \setminus \{0\}$.
- El conjunt $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ de les classes de restes mòdul n és un anell commutatiu amb les operacions heredades de $\mathbb{Z}$. Si considerem l'operació suma, és un grup cíclic generat per la classe de 1. El grup multiplicatiu $\mathbb{Z}_n^*$ és un grup abelià format per les classes dels enters k amb $(k, n) = 1$; el seu cardinal es denota $\varphi(n)$ i vé donat, en termes de la factorització $n = \prod_{i=1}^k p_i^{\alpha_i}$, per la fórmula $\varphi(n) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1)$.
- Sigui K un cos i $n \geqslant 1$. El subconjunt format pels elements $\alpha \in K$ amb $\alpha^n = 1$ és un subgrup de K^* anomenat *subgrup de les arrels n-èsimes de la unitat* de K. Es denota

$\mu_n(K)$. La reunió de tots aquests subgrups és el subgrup de (totes) les arrels de la unitat de K, que es denota $\mu(K)$.

- Sigui K un cos. El conjunt de les matrius $n \times n$ invertibles amb coeficients a K és un grup amb el producte. Es denota $\mathrm{GL}_n(K)$ (grup lineal general). El subconjunt de les matrius de determinant 1 és un subgrup normal, denotat $\mathrm{SL}_n(K)$ (grup especial lineal). Si 1_n denota la matriu identitat $n \times n$, les matrius diagonals del tipus $\alpha 1_n$ amb $\alpha \in K^*$ (homotècies) formen un subgrup (normal) de $\mathrm{GL}_n(K)$. El quocient corresponent es denota $\mathrm{PGL}_n(K)$ (grup projectiu general). El quocient de $\mathrm{SL}_n(K)$ pel subgrup format per les homotècies que conté s'anomena $\mathrm{PSL}_n(K)$ (grup projectiu especial). Tots aquests grups també es poden fabricar a partir d'un anell unitari commutatiu qualsevol.

- Sigui V un K-espai vectorial. El conjunt de les aplicacions lineals invertibles $V \to V$ amb la composició és un grup, anomenat $\mathrm{GL}(V)$ (grup lineal). Quan V és de dimensió finita n, escollir-ne una base equival a establir un isomorfisme $\mathrm{GL}(V) \to \mathrm{GL}_n(K)$.

- Sigui X un conjunt. El conjunt de les aplicacions bijectives de X en ell mateix (permutacions de X), amb la composició forma un grup. Es denota $\mathfrak{S}_X$ o $\mathrm{Perm}\, X$. Si $|X|$ és finit igual a n, aleshores el grup $\mathfrak{S}_X$ conté $n!$ elements. Si $X = \{1, 2, \ldots, n\}$, $\mathfrak{S}_X$ es denota simplement $\mathfrak{S}_n$. El grup $\mathfrak{S}_n$ té un únic subgrup (normal) d'índex 2: el *grup alternat* $\mathfrak{A}_n$ format per les permutacions parelles.

- El conjunt de les isometries del pla $\mathbb{R}^2$ que deixen fix un poligon regular de n costats ($n \geqslant 3$) és un grup, que s'anomena *grup diedral n-èssim* i es denota D_n (o D_{2n}). Està format per les rotacions d'angle $2\pi k/n$, $0 \leqslant k \leqslant n-1$ al voltant del centre del polígon i les simetries respecte d'una recta que uneixi vèrtexs oposats (quan n es parell) o un vèrtex amb el punt mig del costat oposat (quan n és senar). Té cardinal $2n$. Si r denota la rotació amb $k = 1$ i s denota una simetria qualsevol, aleshores $r^n = s^2 = 1$, $sr = r^{-1}s$, i tot element de D_n es pot escriure de manera única com a $s^\alpha r^\beta$ amb $\alpha \in \mathbb{Z}_2$ i $\beta \in \mathbb{Z}_n$.

- El conjunt de les rotacions de $\mathbb{R}^3$ que deixen fix un políedre regular és un grup finit. El grup del tetràedre (quatre triangles) té cardinal 12 i és isomorf a $\mathfrak{A}_4$. El grup del cub (sis quadrats) i el de l'octàedre (vuit triangles) tenen cardinal 24 i són isomorfs a $\mathfrak{S}_4$. El grup del dodecàedre (dotze pentàgons) i l'icosàedre (vint triangles) tenen cardinal 60 i són isomorfs a $\mathfrak{A}_5$. Els grups de les isometries que deixen fixos aquests políedres són isomorfs a $\mathfrak{S}_4$, $\mathfrak{S}_4 \times \mathbb{Z}_2$ i $\mathfrak{A}_5 \times \mathbb{Z}_2$, respectivament.

- Si E és un espai mètric, el conjunt de les isometries $E \to E$ és un grup; anomenem-lo $\mathrm{Isom}\, E$. Si $X \subseteq E$ és un subconjunt, les isometries que deixen fix el conjunt X formen un subgrup de $\mathrm{Isom}\, E$; aquest grup s'anomena *grup de simetria* del conjunt en qüestió. Per exemple, a un triangle isòsceles a $\mathbb{R}^2$ li correspon el grup $\mathbb{Z}_2$; en canvi, una estrella de vuit puntes té grup de simetria més gran (ordre 16), i el grup de simetria d'una circumferència és infinit.

- Sigui A un alfabet (un conjunt finit) de q lletres. Un *codi de bloc* sobre A és un subconjunt no buit $\mathcal{C} \subseteq A^n$ per algun $n \geqslant 1$ (que és la *longitud* del codi). Els vectors

de $\mathcal{C}$ són les *paraules* del codi. Considerem les transformacions sobre un codi de bloc que s'obtenen en fer unes quantes transformacions d'aquests tipus: (1) aplicar una permutació de $\mathfrak{S}_A$ a les lletres d'una posició donada i (2) aplicar una permutació de $\mathfrak{S}_n$ a les coordenades de cada paraula. Les transformacions que deixen fix el codi s'anomenen automorfismes del codi i formen un grup. Els bons codis (en el sentit de la teoria de codis) acostumen a tenir grups d'automorfismes interessants.

3.– El grup simètric

Grups de permutacions. Sigui X un conjunt finit. El conjunt de les permutacions de X (aplicacions bijectives $X \to X$) és un grup amb la composició. El denotarem $\mathfrak{S}_X$ o $\operatorname{Perm} X$.

Si $Y \subseteq X$, podem identificar $\mathfrak{S}_Y$ emb el subgrup de $\mathfrak{S}_X$ format per les permutacions que deixen fixos els elements de $Y \smallsetminus X$.

L'estructura del grup $\mathfrak{S}_X$ queda determinada pel cardinal de X. S'anomena *grup simètric* de n elements el grup de les permutacions del conjunt $X_n = \{1, 2, \ldots, n\}$ i es denota $\mathfrak{S}_n$. Aquest grup té $n!$ elements i si $n \geqslant 3$ no és abelià.

Cicles. Un *cicle* del conjunt X és una família no buida d'elements de X, ordenada llevat d'una permutació cíclica. Per descriure un cicle es fa servir la notació $(a_1, \ldots, a_r)$, tenint en compte que com a cicle és el mateix que $(a_k, \ldots, a_r, a_1, \ldots, a_{k-1})$. El nombre r és la *longitud* del cicle; els cicles de longitud r es diuen, de vegades, r-cicles. Dos cicles $(a_1, \ldots, a_r)$ i $(b_1, \ldots, b_s)$ són *disjunts* si $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \varnothing$.

Tot cicle $(a_1, \ldots, a_r)$ determina una permutació $\sigma \in \mathfrak{S}_X$ definida per

- $\sigma(a_i) = a_{i+1}, \quad 1 \leqslant i \leqslant r-1,$
- $\sigma(a_r) = a_1,$
- $\sigma(a) = a, \quad a \in X \smallsetminus \{a_1, \ldots, a_r\}.$

De fet, el cicle $(a_1, \ldots, a_r)$ s'identifica amb aquesta permutació, de manera que es parla de cicles com a elements de $\mathfrak{S}_X$. Cal anar amb compte amb els 1-cicles, ja que corresponen tots ells a la permutació identitat tot i que com a cicles siguin diferents.

L'ordre d'un r-cicle és r. Els cicles disjunts commuten. Per tant, l'ordre d'un producte de cicles disjunts és el mínim comú múltiple de les seves longituds.

Proposició 3.1. *Tota permutació $\sigma \in \mathfrak{S}_X$ es pot escriure com a producte de cicles disjunts en què apareixen tots els elements de X. Aquesta descomposició és única, llevat de l'ordre d'escriptura dels cicles.*

PROVA: Sigui $\sigma \in \mathfrak{S}_X$. Sigui $a_1 \in X$ qualsevol i considerem els elements

$$a_2 = \sigma(a_1),\ a_3 = \sigma(a_2),\ \ldots,\ a_{i+1} = \sigma(a_i),\ \ldots$$

Com que tots aquests són elements del conjunt finit X, no poden ser tots diferents i arriba un moment que $a_{r+1} \in \{a_1, a_2, \ldots, a_r\}$. Sigui $r \geqslant 1$ l'enter més petit per al qual això passa. Aleshores $a_{r+1} = \sigma(a_r) = a_1$, ja que si $a_{r+1} = a_k$ amb $2 \leq k \leq r$, tindriem $\sigma(a_r) = \sigma(a_{k-1})$ en contradicció amb la injectivitat de σ.

Si $X = \{a_1, \ldots, a_r\}$, $\sigma = (a_1, \ldots, a_r)$ i ja hem acabat. En cas contrari, prenem un altre element $b_1 \in X \setminus \{a_1, \ldots, a_r\}$ i repetim el procés anterior fins a exhaurir els elements de X. Finalment obtindrem una descomposició en cicles disjunts

$$\sigma = (a_1, a_2, \ldots, a_r)(b_1, b_2, \ldots, b_s)\ldots$$

que és òbviament única llevat de l'ordre d'escriptura dels cicles. □

Tipus. El *tipus* d'una permutació vé donat per les longituds dels cicles en què descompon. Es diu que $\sigma \in \mathfrak{S}_n$ és de tipus $[n_1, \ldots, n_k]$ si la seva descomposició consisteix en k cicles disjunts de longituds $n_1, \ldots, n_k$. Naturalment, en tal cas, $n_1 + \cdots + n_k = n$. Una colecció de nombres $n_i \geqslant 1$ tals que $\sum n_i = n$ s'anomena *partició* de n; a $\mathfrak{S}_n$ hi ha permutacions de tants tipus com particions del nombre n.

Si $(a_1, \ldots, a_r)$ és un cicle i σ una permutació qualsevol, és clar que

$$\sigma(a_1, \ldots, a_r)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_r)),$$

de manera que en conjugar un r-cicle s'obté un altre r-cicle. Si $\tau = \gamma_1 \ldots \gamma_k$ és la descomposició en cicles disjunts d'una permutació τ,

$$\sigma\tau\sigma^{-1} = (\sigma\gamma_1\sigma^{-1})\ldots(\sigma\gamma_k\sigma^{-1}),$$

de manera que en conjugar es manté el tipus d'una permutació. És clar també que dues permutacions amb el mateix tipus són sempre conjugades l'una de l'altra. Per tant, el tipus és un invariant de les classes de conjugació que les determina completament.

Transposicions. Una *transposició* és un cicle de longitud 2. Tota permutació es pot descompondre com a producte de transposicions ja que tot cicle descompon com el producte $(a_1, a_2, \ldots, a_r) = (a_1, a_2)(a_2, a_3)\ldots(a_{r-1}, a_r)$.

Lema 3.2. Si $c(\sigma)$ representa el nombre de cicles disjunts en què descompon la permutació σ, i τ és una transposició, $c(\tau\sigma) = c(\sigma) \pm 1$.

PROVA: Sigui $\tau = (a, b)$. Distingim dos casos possibles. En primer lloc, quan a i b apareixen a un mateix cicle de la descomposició de σ, es té

$$\tau\sigma = (a,b)(a,\ldots,x,b,\ldots,y)\gamma_2\ldots\gamma_{c(\sigma)} = (a,\ldots,x)(b,\ldots,y)\gamma_2\ldots\gamma_{c(\sigma)}$$

i, per tant, $c(\tau\sigma) = c(\sigma) + 1$. En segon lloc, quan a i b apareixen a cicles diferents,

$$\tau\sigma = (a,b)(a,\ldots,x)(b,\ldots,y)\gamma_3\ldots\gamma_{c(\sigma)} = (a,\ldots,x,b,\ldots,y)\gamma_3\ldots\gamma_{c(\sigma)}$$

de manera que $c(\tau\sigma) = c(\sigma) - 1$. □

Teorema 3.3. Si $\sigma_1\sigma_2\ldots\sigma_r$ i $\tau_1\tau_2\ldots\tau_s$ són dues descomposicions de la mateixa permutació σ com a producte de transposicions, aleshores r i s tenen la mateixa paritat.

PROVA: Com que σ_r és una transposició, $c(\sigma_r) = n-1$ i, aplicant el lema anterior, obtenim

$$c(\sigma) = c(\sigma_1\ldots\sigma_r) = n - 1\overbrace{\pm 1 \pm 1\cdots\pm 1}^{r-1} = n - 1 + r_1 - (r - 1 - r_1) = n - r + 2r_1,$$

on r_1 és el nombre de signes $+$. Anàlogament tindriem $c(\sigma) = c(\tau_1\ldots\tau_s) = n - s + 2s_1$. Per tant, $n - r + 2r_1 = n - s + 2s_1$ i, en conseqüència, $r \equiv s \pmod 2$. □

Paritat. Grup alternat. Una permutació es diu *parella* o *senar* segons si descompon en un nombre parell o senar de transposicions. Es defineix el *signe* d'una permutació posant $\operatorname{sgn}(\sigma) = +1$ si σ és parella i $\operatorname{sgn}(\sigma) = -1$ si σ és senar. Per tant, $\operatorname{sgn}(\sigma) = (-1)^r$, on r és el nombre de transposicions d'una descomposició de σ.

L'aplicació sgn: $\mathfrak{S}_n \to \{\pm 1\}$ és òbviament un homomorfisme de grups (epimorfisme). El seu nucli està format per les permutacions parelles. S'anomena *grup alternat* i es designa per $\mathfrak{A}_n$. Es tracta d'un subgrup normal de $\mathfrak{S}_n$ i té cardinal $n!/2$.

4.– Estructura

Grups simples. Un grup no trivial es diu *simple* si no té cap subgrup normal propi no trivial; o sigui, si els seus únics subgrups normals són el trivial i el total.

Per exemple, els grups (cíclics) d'ordre primer són simples. És clar que aquests són els únics grups abelians simples.

Siguin G un grup i $H \subseteq G$ un subgrup normal. El quocient G/H és simple si, i només si, H és maximal entre els subgrups normals propis de G.

Teorema 4.1. *Si $n \geqslant 5$ l'alternat $\mathfrak{A}_n$ és simple.*

PROVA: Per veure-ho n'hi ha prou a comprovar els tres fets següents:
- $\mathfrak{A}_n$ està generat per 3-cicles;
- tots els 3-cicles són conjugats a $\mathfrak{A}_n$;
- tot subgrup normal no trivial de $\mathfrak{A}_n$ conté algun 3-cicle.

Tenim que $(a_1, a_2)(a_2, a_3) = (a_1, a_2, a_3)$ i $(a_1, a_2)(a_3, a_4) = (a_1, a_2, a_3)(a_2, a_3, a_4)$. Com que tot element de $\mathfrak{A}_n$ és producte d'un nombre parell de transposicions, els 3-cicles el generen.

Donats 3-cicles (a_1, a_2, a_3) i (b_1, b_2, b_3), sigui $\sigma \in \mathfrak{S}_n$ una permutació amb $\sigma(a_i) = b_i$. Aleshores $\sigma(a_1, a_2, a_3)\sigma^{-1} = (b_1, b_2, b_3)$. Si $\sigma \in \mathfrak{A}_n$ ja hem acabat. En cas contrari, sigui $\tau = (a_4, a_5)$ amb a_4 i a_5 diferents de a_1, a_2, a_3 (això és possible si $n \geqslant 5$). Aleshores la permutació $\sigma\tau$ també envia a_i a b_i i és parella.

Sigui ara H un subgrup normal no trivial de $\mathfrak{A}_n$. Observem que si $\sigma \in H$ i τ és un 3-cicle, $\tau\sigma\tau^{-1}\sigma^{-1} \in H$. Considerem els casos següents, segons la descomposició en cicles disjunts d'un element $\sigma \in H$ no trivial:
- σ té un cicle de longitud $r \geqslant 4$, $\sigma = (a_1, a_2, a_3, a_4, \ldots, a_r)c_2 \cdots c_k$. Sigui τ el 3-cicle (a_1, a_2, a_3). Aleshores $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_3, a_1, a_4, \ldots, a_r)(a_r, \ldots, a_4, a_3, a_2, a_1) = (a_1, a_2, a_4)$, i H conté un 3-cicle.
- σ té dos cicles de longitud 3, $\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)c_3 \cdots c_k$. Sigui $\tau = (a_1, a_2, a_4)$. Tenim $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_4, a_3)(a_1, a_5, a_6)(a_3, a_2, a_1)(a_6, a_5, a_4) = (a_1, a_2, a_5, a_3, a_4)$ i pel cas anterior H conté un 3-cicle.
- σ té un cicle de longitud 3 i la resta de longitud 1 o 2. Aleshores $\sigma^2 \in H$ és un 3-cicle.
- σ descompon en producte de dues transposicions disjuntes, $\sigma = (a_1, a_2)(a_3, a_4)$. Escollim un a_5 diferent de a_1, a_2, a_3, a_4 (possible ja que $n \geqslant 5$). Sigui $\tau = (a_1, a_2, a_5)$. Aleshores $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_5)(a_1, a_2) = (a_1, a_5, a_2)$. Per tant H conté un 3-cicle.
- σ descompon en producte de més de dues transposicions disjuntes, $\sigma = (a_1, a_2)(a_3, a_4)(a_5, a_6)c_4 \cdots c_k$. Sigui $\tau = (a_1, a_2, a_3)$. Aleshores $\tau\sigma\tau^{-1}\sigma^{-1} = (a_2, a_3)(a_1, a_4)(a_1, a_2)(a_3, a_4) = (a_1, a_3)(a_2, a_4)$. Aplicant el cas anterior, H conté un 3-cicle.

Així doncs, tot subgrup normal de $\mathfrak{A}_n$ ($n \geqslant 5$) conté un 3-cicle. Per tant, conté els seus conjugats per elements de $\mathfrak{A}_n$; en particular, conté tots els 3-cicles, de manera que ha de ser tot $\mathfrak{A}_n$. □

Torres de subgrups. Donat un grup G, una *torre normal de subgrups* és una successió

$$G = H_1 \supseteq H_2 \supseteq H_3 \supseteq \cdots \supseteq H_r = 1.$$

on cada H_i és normal a H_{i+1}. Un *refinament* d'una torre normal és una altra torre normal obtinguda intercalant subgrups a la primera. Un refinament és *trivial* quan tots els subgrups afegits ja formaven part de la torre de partida.

S'anomenen *quocients* d'una torre normal els grups H_i/H_{i+1}, $1 \leqslant i \leqslant r-1$. Un refinament trivial afegeix quocients trivials als quocients de la torre de partida.

Dues torres normals de la mateixa longitud es diuen *equivalents* si els seus quocients són isomorfs, llevat d'una permutació.

Una *sèrie de composició* d'un grup G és una torre normal amb $H_i \neq H_{i+1}$ que no admet refinaments no trivials. Clarament, una torre normal és una sèrie de composició si, i només si, els seus quocients són grups simples. Tot grup finit té una sèrie de composició; encara més, qualsevol torre normal formada per subgrups diferents es pot refinar fins una sèrie de composició.

Grups resolubles. Una torre normal es diu *abeliana* (resp. *cíclica*) si els seus quocients són grups abelians (resp. cíclics).

Un grup es diu *resoluble* quan admet una torre normal abeliana. És clar que un grup finit és resoluble si, i només si, tots els quocients de les seves sèries de composició tenen ordre primer.

Proposició 4.2. Els resultats següents es coneixen també, de vegades, com a teoremes d'isomorfisme.

(a) Siguin H i K subgrups normals de G amb $H \subseteq K$. Aleshores $(G/H)/(K/H) \simeq G/K$.

(b) Sigui $f\colon G_1 \to G_2$ un homomorfisme i H_2 un subgrup normal de G_2. Aleshores $H_1 = f^{-1}(H_2)$ és un subgrup normal de G_1 i l'aplicació $f_*(aH_1) = f(a)H_2$ és un monomorfisme $G_1/H_1 \to G_2/H_2$. Si f és epi, f_* és un isomorfisme.

(c) Siguin H i K subgrups de G amb H normal a G. Aleshores $H/(H \cap K) \simeq HK/H$.

(d) Siguin H i K subgrups de G i H_1, K_1 subgrups normals de H i K, respectivament. Aleshores

$$\frac{H_1(H \cap K)}{H_1(H \cap K_1)} \simeq \frac{H \cap K}{(H_1 \cap K)(H \cap K_1)} \simeq \frac{(H \cap K)K_1}{(H_1 \cap K)K_1}$$

PROVA: (a) L'homomorfisme canònic $G \to G/K$ factoritza a través de G/H, ja que $H \subseteq K$, donant $\pi_*\colon G/H \to G/K$ amb $\pi_*(aH) = aK$. Aleshores $\pi_*(aH) = 1 \cdot K \Leftrightarrow aK = K \Leftrightarrow a \in K$, de manera que el el nucli de π_* és K/H.

(b) Composant f amb la projecció canònica tenim un homomorfisme $G_1 \to G_2/H_2$, definit per $a \mapsto f(a)H_2$, que té nucli H_1. Només cal aplicar el teorema d'isomorfisme.

(c) El conjunt HK és un grup i H n'és un subgrup normal. Considerem la composició de la inclusió $K \to HK$ amb la projecció canònica $HK \to HK/H$. Clarament, el nucli d'aquesta aplicació és $H \cap K$ i del teorema d'isomorfisme se'n dedueix el resultat.

(d) Per simetria només cal fer un costat, farem l'esquerre. Considerem els grups $U = H_1(H \cap K_1)$ i $V = H \cap K$. Aleshores $UV = H_1(H \cap K)$, $U \cap V = (H_1 \cap K)(H \cap K_1)$ i V és normal a UV. Aplicant l'apartat anterior, s'obté el resultat. □

Teorema 4.3. (*Teorema de Schreier*). *Dues torres normals d'un grup sempre tenen refinaments equivalents.*

PROVA: Siguin

$$G = H_1 \supseteq H_2 \cdots \supseteq H_r = 1,$$

$$G = K_1 \supseteq K_2 \cdots \supseteq K_s = 1$$

dues torres normals d'un grup G. Considerem els grups

$$H_{i,j} = H_{i+1}(K_j \cap H_i), \quad 1 \leqslant i \leqslant r-1, \quad 1 \leqslant j \leqslant s.$$

Aquests grups són un refinament de la primera torre, doncs

$$H_i = H_{i,1} \supseteq H_{i,2} \supseteq \cdots \supseteq H_{i,s-1} \supseteq H_{i,s} = H_{i+1}.$$

Quan $i < r-1$, $H_{i,s} = H_{i+1} = H_{i+1,1}$, de manera que podem identificar aquests dos grups (però conservarem la doble notació). La longitud del refinament és $(r-1)(s-1)+1$.

Anàlogament, els grups

$$K_{i,j} = K_{j+1}(K_j \cap H_i), \quad 1 \leqslant i \leqslant r, \quad 1 \leqslant j \leqslant s-1,$$

són un refinament de la segona torre. També en aquest cas, per $j < s-1$ és $K_{r,j} = K_{r+1} = K_{r+1,1}$ i, identificant aquests grups, tenim un refinament de longitud $(r-1)(s-1)+1$.

Els dos refinaments construïts són equivalents. En efecte, per i, j amb $1 \leqslant i \leqslant r-1$ i $1 \leqslant j \leqslant s-1$, l'apartat (d) de la proposició anterior proporciona isomorfismes

$$\frac{H_{i,j}}{H_{i,j+1}} = \frac{H_{i+1}(H_i \cap K_j)}{H_{i+1}(H_i \cap K_{j+1})} \simeq \frac{K_{j+1}(H_i \cap K_j)}{K_{j+1}(H_{i+1} \cap K_j)} = \frac{K_{i,j}}{K_{i+1,j}}.$$

□

Corol·lari 4.4. (*Teorema de Jordan-Hölder*). *Totes les sèries de composició d'un grup són equivalents.*

PROVA: Donades dues sèries de composició d'un grup, pel Teorema de Schreier existeixen refinaments equivalents. Pel fet de tractar-se de sèries de composició, aquests refinaments han de ser trivials i no poden afegir-hi nous grups, sinó només repetir grups que ja hi eren. Per tant, els quocients dels refinaments són els quocients de les sèries de composició de partida afegint-hi alguns grups trivials. Com que els refinaments són equivalents, tenen els quocients isomorfs (llevat de l'ordre); en particular els quocients no trivials de l'un i l'altre (que són els de les sèries de composició) són isomorfs. □

Proposició 4.5. *Tot subgrup i tot quocient d'un grup resoluble és resoluble. Una extensió d'un grup resoluble per un grup resoluble és resoluble.*

PROVA: Suposem que G és resoluble i sigui $G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = 1$ una torre abeliana. Si $H \subseteq G$ és un subgrup siguin $H_i = H \cap G_i$; aleshores aplicant l'apartat (b) de la proposició anterior a l'homomorfisme inclusió $H \to G$ tenim monomorfismes de H_i/H_{i+1} en G_i/G_{i+1}. Com que tot subgrup d'un abelià és abelià, H és resoluble. Si K és un quocient de G siguin $K_i = \pi(G_i)$ les imatges dels G_i per la projecció canònica; aleshores el nucli de l'epimorfisme $G_i \to K_i \to K_i/K_{i+1}$ conté G_{i+1}, per tant factoritza a través d'un epimorfisme $G_i/G_{i+1} \to K_i/K_{i+1}$. Com que la imatge homomòrfica d'un grup abelià és abeliana, K és resoluble.

Recíprocament, suposem que H i K són resolubles i que tenim una successió exacta

$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1.$$

Siguin $H = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_r = 1$ i $K = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_s = 1$ torres abelianes. Aleshores considerem la torre de subgrups de G següent:

$$G = g^{-1}(K_1) \supseteq \cdots \supseteq g^{-1}(K_s) = \operatorname{Ker} g = \operatorname{Im} f = f(H_1) \supseteq \cdots \supseteq f(H_r) = 1.$$

Clarament, els quocients d'aquesta torre són els quocients de les dues anteriors; per tant és una torre abeliana. □

Classificació dels grups finits. Pel Teorema de Jordan-Hölder, cada grup finit té associat un conjunt ben determinat de grups simples: els quocients d'una sèrie de composició. Aquest conjunt no determina encara la classe d'isomorfisme del grup. Així el problema de classificar (llevat d'isomorfisme) els grups finits es pot subdividir en dos:

(1) Classificació dels grups simples: trobar tots els grups simples finits.
(2) Problema de les extensions: donats un grup K i un grup simple H, trobar tots els grups G que tenen un subgrup normal H' isomorf a H amb quocient $G/H' \simeq K$.

El primer problema està resolt des de l'any 1980. La solució és el resultat de gairebé cent anys de feina d'una legió de matemàtics i la demostració completa ocupa diversos milers de pàgines d'articles a revistes. El resultat és el següent:

Hi ha 18 famílies infinites de grups simples. Per exemple, tres d'aquestes famílies són
- els grups ciclics d'ordre primer (grups C_p),
- els grups de permutacions parells (grups $\mathfrak{A}_n$) quan $n \geqslant 5$, i
- els grups $\mathrm{PSL}(n,q) = \mathrm{SL}_n(\mathbb{F}_q)/\mathbb{F}_q^*, n \geqslant 2$, excepte si $n = 2$ i $q = 2$ o 3.

Les altres famílies es poden descriure, de manera més o menys complicada, a partir de grups de matrius sobre cossos finits.

A més de les 18 families hi ha 26 grups que no s'engloben a cap d'elles, que s'anomenen *grups esporàdics*. Amb això tenim tots els grups simples finits.

Un dels resultats més importants en el camí d'aquesta demostració és el Teorema de Feit-Thompson (conjectura de Burnside): tot grup finit d'ordre senar és resoluble.

5.– Grups que operen sobre un conjunt

G-conjunts. Siguin G un grup i X un conjunt. Es diu que G *opera* per l'esquerra sobre X si es té una aplicació $G \times X \to X$, que denotarem com un producte $(a, x) \mapsto ax$, tal que $a(bx) = (ab)x$ i $1x = x$. Això també es coneix com *acció* de G sobre X o s'expressa dient que X és un *G-conjunt*.

Per cada $a \in G$ l'aplicació $m_a \colon x \mapsto ax$ és una permutació de X, i l'aplicació $a \mapsto m_a$ és un homomorfisme de G en el grup de permutacions de X. Recíprocament, qualsevol homomorfisme $m \colon G \to \mathfrak{S}_X$, $a \mapsto m_a$, indueix l'acció definida per $ax = m_a(x)$. Per tant, hi ha una bijecció entre les accions de G sobre X (per l'esquerra) i els homomorfismes $G \to \mathfrak{S}_X$.

L'acció es diu *fidel* si elements de G diferents operen sobre X de forma diferent; o sigui, si l'homomorfisme m és injectiu. En aquest cas el grup G es pot identificar amb un subgrup de $\mathfrak{S}_X$.

Hem considerat accions per l'esquerra. Per la dreta tot funciona anàlogament; només cal tenir en compte que les accions per la dreta es corresponen amb els antihomomorfismes $G \to \mathfrak{S}_X$ (o sigui, aplicacions amb $f(ab) = f(b)f(a)$).

Òrbites, punts fixos, estabilitzadors. L'*òrbita* de $x \in X$ és el conjunt Gx; les òrbites formen una partició de X. El conjunt d'òrbites es denota $G\backslash X$ si l'acció és per l'esquerra, X/G si és per la dreta. L'element x és un *punt fix* si la seva òrbita es redueix al propi x; és a dir, si $ax = x$ per tot $a \in G$. L'acció es diu *transitiva* quan per tot parell $x, y \in X$ existeix un $a \in G$ amb $ax = y$; o sigui, quan el conjunt X és una única òrbita.

L'*estabilitzador* d'un element $x \in X$ és el subgrup format pels elements de G que el deixen fix, $G_x = \{a \in G \mid ax = x\}$. També se l'anomena *subgrup d'isotropia* de x. Els estabilitzadors dels elements d'una mateixa òrbita són subgrups conjugats; si $y = ax$ aleshores $G_y = aG_xa^{-1}$.

Si $Y \subseteq X$, l'estabilitzador de Y és el subgrup de G format pels elements que deixen fixos tots els elements de Y; o sigui, la intersecció dels G_x quan x recorre Y. L'estabilitzador de tot X és el subgrup format pels elements que operen trivialment i coincideix amb el nucli de l'homomorfisme associat $m \colon G \to \mathfrak{S}_X$. En particular $\operatorname{Ker} m = \bigcap G_x$.

L'aplicació $ax \mapsto aG_x$ és una bijecció entre l'òrbita d'un $x \in X$ i les classes laterals per l'esquerra del seu estabilitzador G_x. En particular, $|Gx| = |G/G_x|$ i, si G és finit, el nombre d'elements de cada òrbita divideix $|G|$. Quan X és finit tenim la *fórmula de les òrbites*: si $\{x_i\}_{i \in I}$ és una família de representants de les diverses òrbites,

$$|X| = \sum_{i \in I} |Gx_i| = \sum_{i \in I} [G : G_{x_i}].$$

Traslació i conjugació. Tot grup opera sobre ell mateix de dues maneres especialement importants. Per traslació:

$$G \times G \to G \qquad (a, b) \mapsto ab,$$

i per conjugació:

$$G \times G \to G \qquad (a,b) \mapsto aba^{-1}.$$

L'acció per traslació també es pot considerar sobre subconjunts $(a,S) \mapsto aS$ o sobre classes laterals per l'esquerra respecte un subgrup H fixat $(a,bH) \mapsto abH$. En el cas de les classes laterals les accions són sempre transitives, i són fidels si, i només si, $\bigcap_{a\in G} aHa^{-1} = 1$. Quan $H = 1$ tenim una acció fidel del grup G que ens permet veure'l com a grup de permutacions (Teorema de Cayley).

L'acció per conjugació es pot considerar també sobre subconjunts $(a,S) \mapsto aSa^{-1}$ o sobre subgrups de G $(a,H) \mapsto aHa^{-1}$. Les òrbites corresponents són les classes de conjugació (d'un element, subconjunt o subgrup, segons on estem operant). Els subgrups estabilitzadors són els normalitzadors corresponents. En particular, el nombre de conjugats d'un element o subgrup és igual a l'índex del seu normalitzador. El centre d'un grup està format pels punts fixos de l'acció per conjugació sobre elements, i la fórmula de les òrbites, aplicada a aquest cas, diu

$$|G| = |Z(G)| + \sum [G : Z_G(x)],$$

on al sumatori apareixen els índexos dels centralitzadors dels elements que no són del centre; o sigui, els cardinals de les classes de conjugació que contenen més d'un element.

Representacions. Suposem que X és un conjunt amb una estructura determinada i que les permutacions de X que conserven aquesta estructura s'anomenen automorfismes; sigui $\operatorname{Aut} X \subseteq \mathfrak{S}_X$ el subgrup corresponent. Una representació d'un grup G en X (considerat amb l'estructura) és un homomorfisme de grups $\varrho\colon G \to \operatorname{Aut} X$; o sigui, una estructura de G-conjunt sobre X amb la particularitat que les permutacions de X que corresponen als elements de G no són permutacions qualssevol sinó automorfismes. Casos especialment importants són:

- Considerar X simplement com a conjunt. Els automorfismes són les permutacions. Aquest és el cas general que hem tractat d'acció d'un grup sobre un conjunt. Les representacions corresponents s'anomenen *representacions de permutació*.
- Sigui ara $X = A$ un grup abelià. $\operatorname{Aut} A$ està format per les permutacions de A que són homomorfisme de grups. Aquest cas s'estudia a les *representacions de grups*.
- Suposem que $X = V$ té estructura d'espai vectorial sobre un cos K. Els automorfismes de V són aplicacions K-lineals (invertibles) i les representacions són homomorfismes $G \to \mathrm{GL}(V)$. Es diuen *representacions lineals* i són la classe més important de representacions de grups. Quan V és de dimensió finita sobre K, fixant una base podem identificar $GL(V)$ amb $\mathrm{GL}_n(K)$. Per tant, una representació lineal en dimensió finita permet "veure" els elements d'un grup com a matrius.

6.– p-Grups

p-Grups. Sigui p un nombre primer. Un grup finit és un *p-grup* si el seu ordre és una potència de p. Un ***p-subgrup de Sylow*** d'un grup finit G és un subgrup que té per ordre la màxima potència de p que divideix $|G|$.

Teorema 6.1. *Un p-grup no trivial té centre no trivial. En particular, tot p-grup simple és isomorf a $\mathbb{Z}_p$ i tot p-grup és resoluble.*

PROVA: Sigui G un p-grup no trivial. Fem-lo operar sobre ell mateix per conjugació. Per la fórmula de les òrbites,

$$|G| = |Z(G)| + \sum_x [G : G_x].$$

Els índexos $[G : G_x]$ són divisors no trivials de $|G|$. Com que p divideix $|G|$ i també cada $[G : G_x]$, aleshores ha de dividir $|Z(G)|$. Per tant $Z(G)$ és no trivial.

Un p-grup no abelià té, per tant, centre no trivial i diferent del total ja que el centre és un grup abelià. Com que el centre és un subgrup normal el p-grup no és simple.

Una sèrie de composició d'un p-grup té per quocients p-grups, que necessàriament són isomorfs a $\mathbb{Z}_p$; per tant el grup és resoluble. □

Teorema 6.2. (*Teorema de Cauchy*). *Tot grup finit d'ordre divisible per un primer p conté algun element d'ordre p.*

PROVA: Aquest resultat per grups abelians es prova fàcilment. Fem ara el cas general. Ho demostrarem per inducció sobre l'ordre del grup. Considerem G operant sobre si mateix per conjugació. La fórmula de les òrbites diu

$$|G| = |Z(G)| + \sum_x [G : G_x].$$

Si algun dels índexos $[G : G_x]$ és primer amb p tenim un subgrup propi $G_x \subset G$ d'ordre divisible per p que, per hipòtesi d'inducció, conté elements d'ordre p. Si, pel contrari, tots els índexos $[G : G_x]$ són divisibles per p aleshores p divideix l'ordre del centre de G, que és abelià, i conté elements d'ordre p. □

Lema 6.3. *Siguin H un p-subgrup i P un p-subgrup de Sylow d'un grup G. Si $H \subseteq N_G(P)$ aleshores $H \subseteq P$.*

PROVA: Com que $H \subseteq N_G(P)$, $HP = PH$ és un subgrup de G i P n'és un subgrup normal. Aleshores $HP/P \simeq H/H \cap P$ i, per tant, $[HP : P] = [H : H \cap P]$ és una potència de p. Aleshores $|HP| = [HP : P]|P|$ també és una potència de p i, per maximalitat de P, necessariament $HP = P$. Per tant $H \subseteq P$. □

Teorema 6.4. (*Teorema de Sylow*). *Si G és un grup finit d'ordre $p^r n$ amb $(p,n) = 1$, aleshores*

(a) *G té algun p-subgrup de Sylow;*

(b) *tot p-subgrup està contingut dins d'algun p-subgrup de Sylow;*

(c) *tots els p-subgrups de Sylow són conjugats;*

(d) *el nombre de p-subgrups de Sylow divideix n i és congruent amb 1 mòdul p.*

PROVA: (a) Inducció sobre $|G|$. Si $|G| = 1$, $r = 1$ i el subgrup trivial és un p-subgrup de Sylow. Fem operar G sobre ell mateix per conjugació. La fórmula de les òrbites diu

$$|G| = |Z(G)| + \sum_x [G : G_x].$$

Si algun dels índexos $[G : G_x]$ és primer amb p, el grup G_x té ordre $p^r m < p^r n$ amb $(p,m) = 1$ i per hipòtesi d'inducció té p-subgrups de Sylow, que ho són també de G. Suposem que tots aquests índexos són divisibles per p, aleshores també ho és l'ordre del centre $Z(G)$. Sigui a un element d'ordre p a $Z(G)$. El subgrup $\langle a \rangle$ és normal a G, ja que està contingut dins de $Z(G)$. El quocient $G/\langle a \rangle$ té ordre $p^{r-1}n$ i, per hipòtesi d'inducció, té p-subgrups de Sylow. L'antimatge d'un p-subgrup de Sylow de $G/\langle a \rangle$ per la projecció canònica és un p-subgrup de Sylow de G.

(b) Sigui H un p-subgrup i P un p-subgrup de Sylow. Considerem l'acció per conjugació de H sobre el conjunt $\{Q = aPa^{-1} \mid a \in G\}$ dels subgrups conjugats de P. El nombre de conjugats de P és l'índex $[G : N_G(P)]$, que és primer amb p; per la fórmula de classes

$$[G : N_G(P)] = \sum [H : H_Q].$$

Com que els índexos del sumatori son potències de p, algun d'aquests índexos ha de ser 1. Per tant l'acció té punts fixos. Sigui Q un punt fix. Aleshores $H \subseteq N_G(Q)$ i, pel lema anterior, $H \subseteq Q$.

(c) L'argument de l'apartat anterior, en el cas que H és un p-subgrup de Sylow, diu que $H = Q = aPa^{-1}$ per algun a.

(d) Sigui P un p-subgrup de Sylow. Per l'apartat anterior el nombre de p-subgrups de Sylow és igual al nombre de conjugats de P, que és $[G : N_G(P)]$ i divideix n.

Fem operar P sobre el conjunt de p-subgrups de Sylow per conjugació. Si Q és un punt fix d'aquesta acció l'argument de (b) diu que $P = Q$, per tant hi ha un únic punt fix. Per la fórmula de les òrbites, el nombre de subgrups de Sylow és igual a $1 + \sum [P : P_Q]$ i, com que p divideix cadascun dels índexos del sumatori, és $\equiv 1 \pmod{p}$. □

Tema II: ANELLS I MÒDULS

1.– Anells commutatius

Anells, subanells, ideals. Un *anell* és un conjunt amb dues operacions, suma i producte. La suma li dona estructura de grup abelià i el producte és associatiu i distributiu respecte la suma. Si el producte té element neutre, l'anell és *unitari*. Si el producte és commutatiu, l'anell és *commutatiu*. Aqui només considerarem anells unitaris commutatius.

Els elements invertibles d'un anell A formen un grup amb el producte, que es denota A^* i s'anomena *grup multiplicatiu* de l'anell. Quan A és commutatiu, A^* és un grup abelià. Els elements de A^* s'anomenen també *unitats*. Un *cos* és un anell on $1 \neq 0$ i tot element no nul és invertible; o sigui, amb $A^* = A \setminus \{0\}$.

Un *subanell* és un subconjunt d'un anell que amb la restricció de les operacions és un anell. Els subconjunts $\{0,1\}$ i A són subanells de A.

Un *ideal* $\mathfrak{a}$ és un subconjunt que amb la suma és un subgrup i és tancat pel producte per elements de A, $A\mathfrak{a} = \mathfrak{a}$. Tot anell no trivial conté almenys dos ideals: 0 i A. Clarament, $\mathfrak{a} = A \Leftrightarrow \mathfrak{a}$ conté alguna unitat $\Leftrightarrow 1 \in \mathfrak{a}$. El grup quocient $A/\mathfrak{a}$, amb el producte de classes $(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}$, es converteix en un anell.

Dos elements $a, b \in A$ són *congruents* mòdul l'ideal $\mathfrak{a}$ si $a - b \in \mathfrak{a}$; o sigui, si a i b són a la mateixa classe de l'anell quocient $A/\mathfrak{a}$. Es denota $a \equiv b \pmod{\mathfrak{a}}$.

Un *homomorfisme* d'anells $f\colon A \to B$ és un homomorfisme dels grups additius tal que $f(ab) = f(a)f(b)$ i $f(1) = 1$. La imatge i l'antimatge d'un subanell són subanells. L'antimatge d'un ideal és un ideal i, en el cas d'un epimorfisme, la imatge d'un ideal és un ideal. En particular $\operatorname{Im} f = f(A)$ és un subanell de B, $\operatorname{Ker} f = f^{-1}(0)$ és un ideal de A i l'isomorfisme de grups $A/\operatorname{Ker} f \to \operatorname{Im} f$ és un isomorfisme d'anells. Si $\mathfrak{a} \subseteq A$ és un ideal, l'aplicació canònica $\pi\colon A \to A/\mathfrak{a}$ és un epimorfisme d'anells i estableix una bijecció entre els ideals de $A/\mathfrak{a}$ i els ideals de A que contenen $\mathfrak{a}$.

Anells íntegres. Un anell *íntegre* (o *domini*, o *domini d'integritat*) és un anell on $1 \neq 0$ i es compleix la llei de simplificació $ax = ay \Rightarrow x = y$ sempre que $a \neq 0$. Això equival a dir que el producte d'elements no nuls és no nul. Dos elements no nuls amb producte nul s'anomenen *divisors de zero*; un anell és íntegre quan no té divisors de zero. Tot cos és un anell íntegre.

Si A és un anell íntegre el seu *cos de fraccions* és

$$K = \{\, \frac{a}{b} \mid a, b \in A; b \neq 0; \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \,\}.$$

Es comprova immediatament que la suma i producte de fraccions, definits de la manera habitual, donen a K estructura de cos. L'aplicació $a \mapsto a/1$ és un monomorfisme d'anells que permet identificar A amb un subanell de K.

Els anells íntegres es caracteritzen pel fet de ser subanells d'algun cos.

Reticle d'ideals. La intersecció d'una família d'ideals és un ideal. La suma d'ideals $\mathfrak{a} + \mathfrak{b} = \{\, x + y \mid x \in \mathfrak{a},\ y \in \mathfrak{b} \,\}$ és un ideal; també ho és la suma d'una família finita o infinita. Els ideals $\mathfrak{a}$ i $\mathfrak{b}$ s'anomenen *coprimers* (o *relativament primers*) quan $\mathfrak{a} + \mathfrak{b} = A$.

Si S és un subconjunt de l'anell A, l'ideal generat per S és l'ideal més petit de A que conté S. És la intersecció de tots els ideals que contenen S, i està format per tots els elements de la forma $a_1x_1 + \cdots + a_rx_r$ amb $a_i \in A$ i $x_i \in S$. Un ideal és *finitament generat* si està generat per un subconjunt finit, i és *principal* si es pot generar amb un únic element; o sigui, si és de la forma Aa. L'ideal principal generat per a es denota (a) i el generat per una família $a_1, \ldots, a_r$ es denota $(a_1, \ldots, a_r)$.

Donats ideals $\mathfrak{a}$ i $\mathfrak{b}$, definim el seu producte com l'ideal generat pel conjunt producte $\mathfrak{ab}$, i el denotem simplement $\mathfrak{ab}$. Està format pels elements de la forma $x_1y_1 + \cdots + x_ry_r$ amb $x_i \in \mathfrak{a}$ i $y_i \in \mathfrak{b}$. Es defineix anàlogament el producte d'una família finita d'ideals.

En general, $\prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i \subseteq \mathfrak{a}_j \subseteq \sum \mathfrak{a}_i$. Els ideals, amb la inclusió, són un reticle de subconjunts de A, on el suprem és la suma i l'ínfim la intersecció.

Ideals primers i maximals. Un ideal *maximal* és un ideal maximal dins el conjunt dels ideals propis de l'anell. Un ideal *primer* és un ideal $\mathfrak{p} \neq A$ tal que

$$\forall a, b \in A,\ ab \in \mathfrak{p} \ \Rightarrow\ a \in \mathfrak{p} \text{ ó } b \in \mathfrak{p}.$$

Es comprova immediatament que $\mathfrak{m}$ és maximal si, i només si, $A/\mathfrak{m}$ és un cos, i que $\mathfrak{p}$ és primer si, i només si, $A/\mathfrak{p}$ és íntegre. En particular, tot ideal maximal és primer (però el recíproc no és cert). Un anell és un cos si, i només si, 0 és un ideal maximal; i és un domini d'integritat si, i només si, 0 és un ideal primer.

Teorema 1.1. *Tot anell $A \neq 0$ té ideals maximals.*

PROVA: Considerem el conjunt de tots els ideals propis de A, ordenats per inclusió. El conjunt és no buit ja que 0 és un ideal propi de A. Sigui $\{\mathfrak{a}_i\}_{i\in I}$ una cadena d'ideals propis (o sigui, per cada parell $i, j \in I$, $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ ó $\mathfrak{a}_j \subseteq \mathfrak{a}_i$). Aleshores $\mathfrak{a} = \bigcup_{i\in I} \mathfrak{a}_i$ és un ideal propi (és clar pel fet que $\mathfrak{a} = A \Leftrightarrow 1 \in \mathfrak{a}$) que és fita superior de la cadena. Pel lema de Zorn, el conjunt té elements maximals. □

2.– Divisibilitat a un anell íntegre

Divisibilitat. Sigui A un anell íntegre. Un element a *divideix* un element b si existeix un element q amb $b = aq$; es denota $a \mid b$. En termes d'ideals principals, el fet que a divideixi b equival a la inclusió $(b) \subseteq (a)$.

Els elements del grup multiplicatiu A^* es caracteritzen pel fet que divideixen 1, i també perque l'ideal que generen és tot A. S'anomenen *unitats* de l'anell. Si u és una unitat i

$b = au$, els elements a i b s'anomenen *associats*. Ser associats és una relació d'equivalència, que denotarem $a \sim b$. En termes d'ideals principals, $a \sim b \Leftrightarrow (a) = (b)$; per tant, les classes d'elements associats es corresponen amb els ideals principals de l'anell.

L'estudi de la divisibilitat a l'anell A és l'estudi de la relació d'inclusió entre els seus ideals principals. La relació de divisibilitat és un preordre a A, que indueix un ordre al conjunt de les classes d'associats, el qual correspon (intercanviant el sentit) a la inclusió entre els ideals principals.

La relació de divisibilitat s'extén de manera natural al cos de fraccions K de l'anell A. Si $\alpha, \beta \in K$, $\alpha \mid \beta$ si existeix un $q \in A$ tal que $\beta = \alpha q$. La divisibilitat a K no depèn només del cos K sinó de l'anell A (un mateix cos pot ser cos de fraccions d'anells diferents). Es defineix anàlogament el que vol dir que dos elements siguin associats.

Primers. Un element $p \neq 0$, $p \notin A^*$ és *irreductble* si, sempre que $p = ab$, un dels dos elements a ó b és una unitat (i, per tant, l'altre és un associat de p). És a dir, es tracta d'elements de A que només es divideixen per unitats i pels seus associats.

Un element $p \neq 0$, $p \notin A^*$ és *primer* si $p \mid ab \Rightarrow p \mid a$ ó $p \mid b$. Tot element primer és irreductble però el recíproc no és cert. Un element p és primer si, i només si, l'ideal principal (p) és un ideal primer.

Si un element d'un anell descompon en producte de primers, la descomposició és única llevat d'unitats. O sigui, si $p_1 \cdots p_r = q_1 \cdots q_s$ amb p_i i q_j primers, aleshores $r = s$ i, llevat d'una permutació dels índexos, $p_i \sim q_i$.

Màxim comú divisor. Siguin $a, b \in A$. Un *màxim comú divisor* de a i b és un element $d \in A$ tal que per tot $x \in A$,

$$x \mid a \text{ i } x \mid b \quad \Leftrightarrow \quad x \mid d.$$

De manera anàloga es defineix un màxim comú divisor d'una família qualsevol d'elements, finita o infinita. El màxim comú divisor, si existeix, queda determinat llevat d'unitats. És habitual la notació $d = (a, b)$.

Un *mínim comú múltiple* de a i b és un element $m \in A$ tal que per tot $x \in A$,

$$a \mid x \text{ i } b \mid x \quad \Leftrightarrow \quad m \mid x.$$

Es definiex de manera anàloga per famílies amb més de dos elements i, igual que el màxim comú divisor, queda determinat llevat d'unitats. És habitual la notació $m = [a, b]$.

El màxim comú divisor i minim comú multiple d'una família d'elements del cos de fraccions es defineixen anàlogament i, si existeixen, estan definits llevat d'elements de A^*.

Factorització única. Un anell *factorial* (o *domini de factorització única*, abreujat DFU) és un anell on tot element no nul descompon en un producte

$$a = \prod_{i=1}^{r} p_i^{m_i}$$

amb p_i irreductbles diferents (no associats) i $m_i > 0$ de manera única; o sigui, si $a = \prod_{j=1}^{s} q_j^{n_j}$ n'és una altra descomposició, necessàriament $r = s$ i, llevat d'una permutació dels índexos, $p_i \sim q_i$ i $m_i = n_i$.

Es comprova fàcilment que a un DFU els elements irreductbles són primers.

Sigui p un primer de A. Per cada $a \in A$ no nul definim $\operatorname{ord}_p a = m \geqslant 0$ si $p^m \mid a$ i $p^{m+1} \nmid a$. Definim $\operatorname{ord}_p 0 = \infty$. Llavors,

- $\operatorname{ord}_p(ab) = (\operatorname{ord}_p a)(\operatorname{ord}_p b)$ i
- $\operatorname{ord}_p(a+b) \geqslant \min\{\operatorname{ord}_p a, \operatorname{ord}_p b\}$, amb igualtat si $\operatorname{ord}_p a \neq \operatorname{ord}_p b$.

Sigui $\mathbb{P}$ una família de representants de les classes de primers associats (si $A = \mathbb{Z}$ s'acostuma a escollir els primers positius i si $A = K[X]$ els polinomis mònics). Aleshores tot element no nul $a \in A$ s'escriu de manera única com

$$a = u \prod_{p \in \mathbb{P}} p^{\operatorname{ord}_p a},$$

amb $u \in A^*$, tenint en compte que els exponents $\operatorname{ord}_p a$ són zero llevat d'un nombre finit. La relació de divisibilitat es tradueix en

$$a \mid b \quad \Leftrightarrow \quad \forall p \in \mathbb{P},\ \operatorname{ord}_p a \leqslant \operatorname{ord}_p b.$$

Tota família $\{a_i\}$ d'elements de A té un màxim comú divisor d i, si és finita, un mínim comú múltiple m, determinats per

$$\operatorname{ord}_p d = \min\{\operatorname{ord}_p a_i\} \qquad \text{i} \qquad \operatorname{ord}_p m = \max\{\operatorname{ord}_p a_i\}.$$

Factorització al cos de fraccions. Si A és un DFU i K el seu cos de fraccions, la factorització única s'extén de manera natural a K en el sentit que tot element no nul $\alpha \in K$ s'escriu, de manera única, com un producte

$$\alpha = u \prod_{p \in \mathbb{P}} p^{m_p}$$

amb $u \in A^*$ una unitat i exponents $m_p \in \mathbb{Z}$ quasi tots zero.

Extenem ord_p a K definint $\operatorname{ord}_p(a/b) = \operatorname{ord}_p a - \operatorname{ord}_p b$. A la descomposició anterior, $\operatorname{ord}_p \alpha = m_p$. Es comprova immediatament que ord_p està ben definida i que proporciona un homomorfisme de grups $K^* \to \mathbb{Z}$; el nucli d'aquest homomorfisme és A^* i l'antimatge de $\mathbb{N}$ és $A \setminus \{0\}$. Les propietats de ord_p a A enunciades més amunt també valen a K.

També al cos de fraccions, la divisibilitat es tradueix en

$$\alpha \mid \beta \quad \Leftrightarrow \quad \forall p \in \mathbb{P},\ \operatorname{ord}_p \alpha \leqslant \operatorname{ord}_p \beta;$$

i el màxim comú divisor $d \in K$ i mínim comú múltiple $m \in K$ d'una família finita $\{\alpha_i\}$ d'elements de K queden determinats per

$$\operatorname{ord}_p d = \min\{\operatorname{ord}_p \alpha_i\} \qquad \text{i} \qquad \operatorname{ord}_p m = \max\{\operatorname{ord}_p \alpha_i\}.$$

A més, el fet que tots els α_i siguin elements de l'anell A (tinguin unitats al denominador) equival a què $d \in A$.

Anells principals. Un anell *principal* (o *domini d'ideals principals*, abreujat DIP) és un anell íntegre en què tot ideal és principal.

A un DIP, el màxim comú divisor d i el mínim comú múltiple m dels elements $a_1, \ldots, a_n$ queden determinats per

$$(d) = (a_1, \ldots, a_n), \qquad (m) = (a_1) \cap \cdots \cap (a_n).$$

Teorema 2.1. *Tot domini d'ideals principals és un anell factorial.*

PROVA: Primer de tot observem que tota cadena ascendent d'ideals de A estabilitza; o sigui que, donats $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ existeix un n tal que $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$ En efecte, sigui $\mathfrak{a} = \bigcup \mathfrak{a}_i$; clarament $\mathfrak{a}$ és un ideal que, com tots els de A, és principal. Sigui $\mathfrak{a} = (a)$; aleshores $a \in \mathfrak{a}_n$ per algun n i, per tant, $\mathfrak{a}_n = \mathfrak{a}$, de manera que $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots = \mathfrak{a}$.

Suposem que existeix un element $a \in A$ no trivial que no factoritza en producte d'irreductbles. Això vol dir que existeix alguna factorització $a = a_1 b_1$ en què a_1 i b_1 no són unitats i almenys un dels dos no factoritza en producte d'irreductbles. Suposem que és a_1. Aleshores $a_1 = a_2 b_2$ amb un dels dos (diguem a_2) que no factoritza en producte d'irreductbles i b_2 no unitat. Repetint l'argument obtenim una successió $a = a_0, a_1, a_2, \ldots$ tal que $a_{i+1} \mid a_i$ però $a_i \nmid a_{i+1}$, i la cadena d'ideals $(a_0) \subset (a_1) \subset (a_2) \subset \ldots$ no estabilitza. Contradicció.

Per veure que la factorització és única n'hi ha prou a comprovar que els irreductbles són, de fet, primers. Sigui p un irreductble. Si $(p) \subseteq (a)$, $p = ax$ per algún x i, per tant, a és un associat de p ($\Rightarrow (a) = (p)$) o bé a és una unitat ($\Rightarrow (a) = A$). Aleshores (p) és un ideal maximal, per tant primer, i p és un element primer. □

Anells euclidians. Una *norma euclidiana* a un anell íntegre A és una aplicació

$$N \colon A \setminus \{0\} \to \mathbb{N}$$

tal que, per tot parell $a, b \in A$ amb $b \neq 0$, existeixen elements q i r tals que $a = bq + r$ i $N(r) < N(b)$ o $r = 0$. En aquest cas, l'expresió $a = bq + r$ s'anomena *divisió euclidiana* de a per b i els elements q i r són el *quocient* i el *reste* de la divisió euclidiana.

Siguin a i b amb $b \neq 0$. L'*algoritme d'Euclides* consisteix a efectuar divisions euclidianes successives segons l'esquema següent: siguin $r_0 = a$ i $r_1 = b$ i, mentre $r_k \neq 0$, siguin q_k i r_{k+1} tals que

$$r_{k-1} = r_k q_k + r_{k+1}, \quad r_{k+1} = 0 \ \text{ó} \ N(r_{k+1}) < N(r_k).$$

Així es va obtenint una successió de restes $r_0, r_1, r_2, \ldots$ amb $N(r_1) > N(r_2) > \ldots$. Com que no pot ser que les normes d'aquests restes, que són nombres naturals, decreixin indefinidament, aquest procés és necessàriament finit. O sigui, arriba un moment que la divisió dóna reste zero.

Teorema 2.2. *Tot anell euclidià és principal.*

PROVA: Sigui $\mathfrak{a}$ un ideal no trivial de A. Sigui $a \in \mathfrak{a}$ un element no nul de norma mínima. Vegem que $\mathfrak{a} = (a)$. Donat $x \in \mathfrak{a}$, considerem la divisió euclidiana $x = aq + r$. Com que $r = x - aq \in \mathfrak{a}$ i a és no nul amb norma mínima, $r = 0$ i $x \in \mathfrak{a}$. □

Càlculs explícits a un anell euclidià. Els anells euclidians tenen l'avantatge que, si sabem fer explícitament la divisió euclidiana, és fàcil calcular el màxim comú divisor de dos elements. En efecte, és trivial comprovar que donats $a, b \in A$ amb $b \neq 0$, l'últim reste no nul de l'algoritme d'Euclides és màxim comú divisor de a i b.

D'altra banda, també resulta fàcil resoldre la *identitat de Bézout*: donats $a, b \in A$ no tots dos nuls, sigui d el seu màxim comú divisor. Aleshores es té la igualtat d'ideals $(a, b) = (d)$ i existeixen elements $x, y \in A$ tals que $ax + by = d$. Per trobar-los explícitament es defineixen, a partir dels quocients de l'algoritme d'Euclides, les successions

$$\begin{array}{lll} x_0 = 1, & x_1 = 0, & x_{k+1} = x_{k-1} - q_k x_k; \\ y_0 = 0, & y_1 = 1, & y_{k+1} = y_{k-1} - q_k y_k. \end{array}$$

Es comprova, per inducció, que $ax_k + by_k = r_k$ i, en particular, quan r_n és l'últim reste no nul, s'obté una solució de la identitat de Bézout.

Exemples

- *Els nombres enters.* $\mathbb{Z}$ és un anell euclidià amb norma euclidiana el valor absolut: donats enters a i $b \neq 0$ existeixen enters q i r amb $a = bq + r$ i $|r| < |b|$; els enters q i r no queden unívocament determinats (en general hi ha dos parells possibles) però si que ho estan si imposem que $0 \leqslant r < |b|$ (reste positiu mínim) o que $-|b|/2 < r \leqslant |b|/2$ (reste amb valor absolut mínim). Les unitats de $\mathbb{Z}$ són $\{\pm 1\}$. Els associats de $n \neq 0$ són $\pm n$; si escollim el positiu com a representant canònic, cada enter no nul s'escriu de manera única com un producte $\pm \prod p_i^{m_i}$ on els p_i són nombres primers positius.

- *Els polinomis en una variable.* Sigui K un cos. L'anell $K[X]$ és un anell euclidià amb norma euclidiana el grau: donats polinomis $f(X)$ i $g(X) \neq 0$ existeixen dos únics polinomis $q(X)$ i $r(X)$ amb $f(X) = g(X)q(X) + r(X)$ i r de grau estrictament menor que g. Les unitats de $K[X]$ són els elements de K^*. Els associats d'un $f(X) \neq 0$ s'obtenen multiplicant-lo per constants no nul·les, i cada classe d'associats conté un únic polinomi mònic. Tot polinomi no nul s'escriu de manera única com un producte $u \prod p_i(X)^{m_i}$ on u és una constant no nul·la i $p_i(X)$ són polinomis mònics irreductbles.

- *Els enters dels cossos quadràtics imaginaris.* Sigui $m < 0$ un enter lliure de quadrats. Siguin

$$w = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \pmod 4, \\ (1 + \sqrt{m})/2, & m \equiv 1 \pmod 4; \end{cases} \qquad D = \begin{cases} 4m, & m \equiv 2, 3 \pmod 4, \\ m, & m \equiv 1 \pmod 4. \end{cases}$$

Sigui $A = \mathbb{Z}[w]$ l'anell format pels nombres complexos de la forma $a+bw$ amb $a, b \in \mathbb{Z}$. Definim l'aplicació norma $N\colon A \to \mathbb{Z}$, $N(z) = z\overline{z} = |z|^2$. Aleshores (ull, algunes d'aquestes afirmacions estan molt lluny de ser trivials);

- A és un anell euclidià si, i només si, $D = -3, -4, -7, -8, -11$. En aquest cas l'aplicació norma és una norma euclidiana.
- A és un anell factorial si, i només si, $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Sigui $p \in \mathbb{Z}$ un nombre primer. Si D no és un residu quadràtic mòdul p, aleshores p és primer a A. Si D és un residu quadràtic mòdul p, existeixen dos primers diferents $\mathfrak{p}_1$ i $\mathfrak{p}_2$ a A tals que $\mathfrak{p}_1\mathfrak{p}_2 = p$. Si p divideix D, existeix un primer $\mathfrak{p}$ a A tal que $\mathfrak{p}^2 = p$.
- Les unitats de l'anell A són ± 1 excepte si $D = -3$, que n'hi ha sis (les arrels sisenes de la unitat), i si $D = -4$, que n'hi ha quatre (les arrels quartes de la unitat).
- Per als altres valors de D, l'anell A no és factorial. Tot element factoritza en producte d'irreductbles pero la factorització no sempre és única. En canvi, tot ideal factoritza de manera única en producte d'ideals primers. De fet, la paraula *ideal* prové d'una situació com aquesta: quan entre els elements de l'anell no hi ha factorització única, es construeixen uns altres objectes, els "ideals", on si que hi ha factorització única, i els elements de l'anell en són un cas particular (els ideals principals).

3.– Polinomis en una variable

Polinomis sobre un cos. Sigui K un cos. L'anell de polinomis en una variable és

$$K[X] = \{f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \mid a_i \in K\}$$

amb les operacions suma i producte habituals. Si $a_n \neq 0$ el polinomi $f(X)$ té *grau* n, es denota $\deg f = n$. Per definició, $\deg 0 = -\infty$. El grau compleix les propietats

- $\deg fg = \deg f + \deg g$,
- $\deg(f+g) \leqslant \max\{\deg f, \deg g\}$, amb igualtat si $\deg f \neq \deg g$;

i proporciona una norma euclidiana a l'anell de polinomis: donats polinomis f i g, $g \neq 0$, existeixen polinomis q i r amb $f = gq + r$ i $\deg r < \deg g$; a més, q i r són únics.

Els polinomis invertibles a $K[X]$ són les constants no nul·les. Un polinomi amb $a_n = 1$ es diu mònic. Tot polinomi és associat d'un únic polinomi mònic; per tant, els polinomis mònics són generadors canònics dels ideals no nuls. Un polinomi irreductble (o primer) és un polinomi no constant que no factoritza en producte de polinomis de grau estrictament menor; en particular tots els polinomis de grau 1 són irreductbles. Tot polinomi no nul

factoritza de manera única com una constant no nul·la per un producte de polinomis mònics irreductbles.

L'anell $K[X]$ conté infinits polinomis primers. Per provar-ho es pot fer servir el mateix argument d'Euclides que demostra la infinitud dels nombres primers.

Arrels. A cada element $\alpha \in K$ li correspon un únic homomorfisme d'anells $K[X] \to K$ que envia les constants a elles mateixes i X a α. Denotem $f(\alpha)$ la imatge del polinomi $f(X)$ per aquest homomorfisme, i ho interpretem com el *valor* del polinomi f *avaluat* a l'element α. L'element α és una *arrel* de f si $f(\alpha) = 0$; això equival a dir que el polinomi primer $X - \alpha$ divideix $f(X)$. Si $f(X) = (X-\alpha)^m g(X)$ i $X - \alpha$ no divideix $g(X)$, α és una arrel de $f(X)$ de *multiplicitat* $m \geqslant 0$; és el mateix que dir que $f(X)$ té ordre m al primer $X - \alpha$. Una *arrel múltiple* és una arrel de multiplicitat > 1.

Si K és un subcos d'un cos L, podem avaluar els polinomis de $K[X]$ a un element $\alpha \in L$ obtenint un homomorfisme $K[X] \to L$. L'element α és *trascendent* sobre K si aquest homomorfisme és injectiu i és *algebraic* en cas contrari, o sigui, quan és arrel d'algun polinomi no nul de $K[X]$.

Derivació. Si $f(X) = \sum_{i=0}^{n} a_i X^i$, la seva *derivada* és el polinomi $f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$. Valen les fórmules $(f+g)' = f'+g'$, $(fg)' = f'g+fg'$, $(f^k)' = kf'f^{k-1}$. D'aquestes fórmules es dedueix que si $f(X) = \prod p_i(X)^{m_i}$ és la factorització del polinomi f, $\prod p_i(X)^{m_i-1}$ divideix el màxim comú divisor de f i f'. Les arrels múltiples d'un polinomi són les arrels comunes del polinomi i la seva derivada.

Polinomis sobre un anell factorial. Sigui A un anell factorial i K el seu cos de fraccions. L'anell $A[X]$ format pels polinomis amb coeficients a A està contingut dins de $K[X]$. Sigui $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. Definim el *contingut* de f com el màxim comú divisor dels coeficients $a_0, \ldots, a_n$, i el denotem $\operatorname{cont} f$. Un polinomi $f(X) \in K[X]$ té coeficients a l'anell A si, i només si, el seu contingut és un element de A. Naturalment, el contingut està definit llevat d'unitats.

Un polinomi *primitiu* és un polinomi amb contingut 1 (o una unitat). Els polinomis primitius tenen coeficients a l'anell A. Es caracteritzen per tenir els coeficients coprimers.

Si $\alpha \in K$ és una constant, $\operatorname{cont} \alpha f = \alpha \operatorname{cont} f$. Tot polinomi no nul $f(X) \in K[X]$ descompon en producte $f(X) = (\operatorname{cont} f) f_1(X)$ amb $f_1(X) \in A[X]$ primitiu, i aquesta descomposició (com a producte d'una constant per un polinomi primitiu) és única, llevat d'unitats.

Teorema 3.1. (*Lema de Gauss*). *El producte de polinomis primitius és primitiu.*

PROVA: Siguin $f(X) = \sum_{i=0}^{n} a_i X^i$ i $g(X) = \sum_{i=0}^{m} b_i X^i$ polinomis primitius, i sigui $f(X)g(X) = \sum_{i=0}^{n+m} c_i X^i$.

Donat un primer p, sigui $0 \leqslant r \leqslant n$ l'enter més petit tal que $p \nmid a_r$ i $0 \leqslant s \leqslant m$ l'enter més petit tal que $p \nmid b_s$. Aleshores p no divideix c_{r+s}, ja que

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + a_{r-1} b_{s+1} + \cdots + a_{r+1} b_{s-1} + \cdots$$

i, apart de $a_r b_s$, que no és divisible per p, cada sumand conté un factor a_i amb $i < r$ o un factor b_j amb $j < s$, que són divisibles per p. Per tant, p no divideix el màxim comú divisor dels coeficients de $f(X)g(X)$. Com que això és cert per tot primer p, $f(X)g(X)$ és primitiu. □

Corol·lari 3.2. *Sigui A un anell factorial i K el seu cos de fraccions. Aleshores:*
(a) *si $f, g \in K[X]$, $\operatorname{cont}(fg) \simeq (\operatorname{cont} f)(\operatorname{cont} g)$;*
(b) *si $f, g, h \in A[X]$, $f = gh$ i f és primitiu, g i h també són primitius;*
(c) *si $f \in A[X]$ és primitiu, f és irreductble a $A[X]$ si, i només si, ho és a $K[X]$.*

PROVA: (a) Siguin $f = c_f f_1$ i $g = c_g g_1$, amb f_1 i g_1 primitius. Aleshores $fg = c_f c_g f_1 g_1$. Pel lema de Gauss $f_1 g_1$ és primitiu, i $\operatorname{cont}(fg) = c_f c_g$ llevat d'unitats.

(b) $\operatorname{cont} f = (\operatorname{cont} g)(\operatorname{cont} h)$. Si $\operatorname{cont} f$ és una unitat, els altres dos també ho són.

(c) Si $f = gh$ és una descomposició no trivial a $A[X]$, g i h no poden ser constants ja que dividirien el contingut de f, que és una unitat. Per tant, aquesta descomposició és no trivial a $K[X]$. Recíprocament, si $f = gh$ és una descomposició no trivial a $K[X]$, g i h són no constants. Treient-los-hi el contingut $f = c_g c_h g_1 h_1$, $c_g c_h$ és una unitat i aquesta és una descomposició no trivial a $A[X]$. □

Teorema 3.3. *Si A és un anell factorial i K el seu cos de fraccions, aleshores l'anell de polinomis $A[X]$ també és factorial i els primers de $A[X]$ són els primers de A i els polinomis primitius irreductbles a $K[X]$.*

PROVA: Ja hem vist que els polinomis primitius són irreductbles a $A[X]$ si, i només si, ho són a $K[X]$. És clar que una constant és irreductble a $A[X]$ si, i només si, ho és a A.

Donat $f(X) \in A[X]$ no nul considerem una factorització a l'anell $K[X]$, $f(X) = cp_1(X) \cdots p_r(X)$, amb $c \in K^*$ i p_i polinomis irreductbles a $K[X]$. Treient-los el contingut i afegint-lo a la constant, podem suposar que els $p_i(X)$ tenen contingut 1 i, per tant, són polinomis irreductbles de $A[X]$. Sigui $c = q_1 \cdots q_s$ una factorització a A. Aleshores $f(X) = q_1 \cdots q_s p_1(X) \cdots p_r(X)$ és una factorització de $f(X)$ en irreductbles de $A[X]$.

La unicitat és immediata. □

Polinomis en diverses variables. L'anell de polinomis en diverses variables es pot definir inductivament com $K[X_1, \ldots, X_n] = K[X_1, \ldots, X_{n-1}][X_n]$. Pel teorema anterior, aquest anell és un DFU. Per $n \geqslant 2$ no és un DIP; en efecte, és clar que l'ideal generat per $X_1, \ldots, X_n$ no és principal.

Teorema 3.4. (*Criteri d'irreductbilitat d'Eisenstein*). *Sigui A un anell factorial i K el seu cos de fraccions. Sigui $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ un polinomi no constant. Si existeix un primer p de A tal que*

$$\operatorname{ord}_p a_n = 0, \quad \operatorname{ord}_p a_0 = 1, \quad \operatorname{ord}_p a_i > 0,\ i = 1, \ldots, n-1,$$

aleshores f és irreductble a $K[X]$.

PROVA: Pel lema de Gauss, si f factoritza a $K[X]$ també ho fa a $A[X]$. Suposem que $f(X) = g(X)h(X)$ amb $g(X) = \sum_{i=0}^{r} b_iX^i$ i $h(X) = \sum_{i=0}^{s} c_iX^i$ polinomis de $A[X]$ no constants. En particular, $r < n$ i $s < n$. Els coeficients b_r i c_s no són divisibles per p ja que $a_n = b_rc_s$ i $\operatorname{ord}_p a_n = 0$. Dels coeficients b_0 i c_0 l'un és divisible per p i l'altre no, ja que $a_0 = b_0c_0$ i $\operatorname{ord}_p a_0 = 1$; suposem que b_0 és divisible per p. Sigui $1 \leqslant t \leqslant r$ l'enter més petit tal que $p \nmid b_t$. Aleshores p no dividiex a_t ja que

$$a_t = b_tc_0 + b_{t-1}c_1 + \ldots$$

i p no divideix el sumand b_tc_0 mentre que divideix els altres sumands. Això contradiu la hipòtesi sobre la divisibilitat dels a_i. □

Teorema 3.5. (*Criteri d'irreductbilitat per reducció*). *Sigui A un anell factorial amb cos de fraccions K, sigui p un primer de A i sigui L el cos de fraccions de l'anell íntegre $A/(p)$. Considerem la projecció canònica $\pi\colon A \to A/(p)$. Donat un polinomi $f(X) = \sum_{i=0}^{n} a_iX^i \in A[X]$ diguem $f^\pi(X) = \sum_{i=0}^{n} \pi(a_i)X^i$. Aleshores, si $p \nmid a_n$ i f^π és irreductble a $L[X]$, f és irreductble a $K[X]$.*

PROVA: En efecte, qualsevol descomposició no trivial $f(X) = g(X)h(X)$ hauria de tenir lloc a $A[X]$ (pel lema de Gauss) i els coeficients de grau més gran de g i h no es dividirien per p. En tal cas, els polinomis f^π, g^π i h^π tindrien el mateix grau que f, g i h respectivament i la identitat $f^\pi(X) = g^\pi(X)h^\pi(X)$ seria una descomposició no trivial de f^π a l'anell $A/(p)$ i, per tant, al seu cos de fraccions. □

4.– Polinomis simètrics

Polinomis en diverses variables. Sigui A un anell (commutatiu, unitari) qualsevol. L'anell de polinomis en diverses variables amb coeficients a A es pot definir per recurrència:

$$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n].$$

A la secció anterior hem vist que quan A és un cos (o simplement un anell factorial) aquest és un anell factorial

El grau d'un monomi $X_1^{\nu_1} \cdots X_n^{\nu_n}$ és $\nu_1 + \cdots + \nu_n$, i el grau d'un polinomi és el màxim dels graus dels monomis que hi apareixen amb coeficient no nul.

Sigui A un subanell de B. A cada n-pla $(\alpha_1, \ldots, \alpha_n)$ d'elements de B li correspon un (únic) homomorfisme d'anells $A[X_1, \ldots, X_n] \to B$ que envía les constants a elles mateixes i cada X_i a α_i. Denotem $f(\alpha_1, \ldots, \alpha_n)$ la imatge del polinomi $f(X_1, \ldots, X_n)$ per aquest homomorfisme, i ho interpretem com el el *valor* del polinomi f *avaluat* als elements α_i. Els α_i són *algebraicament independents* sobre l'anell A si l'homomorfisme anterior és injectiu; o sigui, si l'únic polinomi que s'anul·la als α_i és el polinomi zero.

Polinomis simètrics. Per cada $\sigma \in \mathfrak{S}_n$ i $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ definim f^σ com el polinomi

$$f^\sigma(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Es tracta del polinomi que hom obté en permutar les variables al polinomi f segons la permutació σ. Valen les fórmules $(f+g)^\sigma = f^\sigma + g^\sigma$ i $(fg)^\sigma = f^\sigma g^\sigma$ i, per tant, el que tenim és una acció de $\mathfrak{S}_n$ sobre l'anell $A[X_1, \ldots, X_n]$. Els punts fixos d'aquesta acció s'anomenen *polinomis simètrics* i són un subanell de $A[X_1, \ldots, X_n]$. Per exemple,

$$S_1 = S_1(X_1, \ldots, X_n) = \sum_i X_i = X_1 + X_2 + \cdots + X_n$$

$$S_2 = S_2(X_1, \ldots, X_n) = \sum_{i<j} X_i X_j = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n$$

$$\ldots$$

$$S_k = S_k(X_1, \ldots, X_n) = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k}$$

$$\ldots$$

$$S_n = S_n(X_1, \ldots, X_n) = X_1X_2 \cdots X_n$$

ho són, s'anomenen *polinomis simètrics elementals* en les variables $X_1, \ldots, X_n$ i es relacionen amb les variables a través de la identitat

$$(X - X_1)(X - X_2) \cdots (X - X_n) = X^n - S_1X^{n-1} + S_2X^{n-2} + \cdots + (-1)^n S_n.$$

Sigui $f(X) \in K[X]$ un polinomi en una variable,

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = a_0(X - \alpha_1) \cdots (X - \alpha_n).$$

Els polinomis simètrics elementals ens proporcionen els coeficients del polinomi f en termes de les seves arrels:

$$a_k = (-1)^k a_0 S_k(\alpha_1, \ldots, \alpha_n).$$

Teorema 4.1. (*Teorema fonamental dels polinomis simètrics*). *Si f és un polinomi simètric en les variables $X_1, \ldots, X_n$, existeix un polinomi g en n variables tal que*

$$f(X_1, \ldots, X_n) = g(S_1, \ldots, S_n),$$

on els S_k són els polinomis simètrics elementals en les variables X_i.

PROVA: Definim el *pes* d'un monomi en n variables $T_1^{\nu_1} \cdots T_n^{\nu_n}$ com $\nu_1 + 2\nu_2 + \cdots + n\nu_n$ i el pes d'un polinomi en $T_1, \ldots, T_n$ com el màxim dels pesos dels monomis que hi intervenen. Si g és un polinomi en n variables, el grau de $g(S_1, \ldots, S_n)$ com a polinomi en les variables $X_1, \ldots, X_n$ és menor o igual que el pes de g.

Donat un polinomi simètric $f(X_1, \ldots, X_n)$ de grau d, demostrarem que existeix un polinomi g com es demana a l'enunciat que, a més, té pes $\leqslant d$. La demostració és per inducció, primer sobre el nombre de variables n, i després sobre el grau d.

Si $n = 1$ és trivial ja que $S_1 = X_1$, el pes és el grau, i podem prendre $g = f$. Suposem-ho demostrat per $n-1$ variables. Si $d = 0$, f és constant i el resultat és trivial. Suposem-ho demostrat per grau $\leqslant d - 1$. El poliniomi $f(X_1, \ldots, X_{n-1}, 0)$ és un polinomi simètric en $n-1$ variables. Per hipòtesi d'inducció (sobre el nombre de variables) existeix un polinomi g_1 en $n-1$ variables de pes $\leqslant d$ tal que

$$f(X_1, \ldots, X_{n-1}, 0) = g_1(S'_1, \ldots, S'_{n-1}),$$

on S'_k és el k-èsim polinomi simètric elemental en les variables $X_1, \ldots, X_{n-1}$. El polinomi $g_1(S_1, \ldots, S_{n-1})$ té grau $\leqslant d$ en les variables $X_1, \ldots, X_n$, i el polinomi

$$f_1(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - g_1(S_1, \ldots, S_{n-1}),$$

és un polinomi simètric de grau $\leqslant d$. Com que $f_1(X_1, \ldots, X_{n-1}, 0) = 0$, f_1 es divideix per X_n i, per simetria, per cadascuna de les variables X_i. Sigui f_2 tal que $f_1 = X_1 \cdots X_n f_2 = S_n f_2$. El polinomi f_2 és simètric en n variables i té grau $d - n < d$. Per hipòtesi d'inducció (sobre el grau) existeix un polinomi g_2 en n variables de pes $\leqslant d - n$ tal que $f_2(X_1, \ldots, X_n) = g_2(S_1, \ldots, S_n)$. Aleshores

$$f(X_1, \ldots, X_n) = g_2(S_1, \ldots, S_n)S_n + g_1(S_1, \ldots, S_{n-1})$$

i l'expresió de la dreta és un polinomi en $S_1, \ldots, S_n$ de pes $\leqslant d$. □

Teorema 4.2. *Les funcions simètriques elementals són algebraicament independents (l'afirmació equival a la unicitat del polinomi g del teorema anterior).*

PROVA: Per inducció sobre n. Per $n = 1$ és la mateixa definició d'un anell de polinomis en una variable. Suposem-ho provat per les funcions simètriques elementals en $n-1$ variables.

Suposem que les funcions simètriques en n variables admeten una relació algebraica no trivial. Sigui g un polinomi en n variables de grau mínim tal que $g(S_1, \ldots, S_n) = 0$. Escrivim g com a polinomi en l'última de les seves variables

$$g(T_1, \ldots, T_n) = g_0(T_1, \ldots, T_{n-1}) + g_1(T_1, \ldots, T_{n-1})T_n + \cdots + g_d(T_1, \ldots, T_{n-1})T_n^d.$$

El polinomi g_0 no pot ser el polinomi zero ja que si ho fos tindriem $g(S_1,\ldots,S_n) = S_n h(S_1,\ldots,S_n) = 0$ amb h de grau estrictament menor que el de g. Substituïnt a l'expressió anterior T_i per S_i, queda

$$0 = g_0(S_1,\ldots,S_{n-1}) + g_1(S_1,\ldots,S_{n-1})S_n + \cdots + g_d(S_1,\ldots,S_{n-1})S_n^d,$$

i avaluant a $X_n = 0$ s'obté

$$0 = g_0(S'_1,\ldots,S'_{n-1}),$$

on les S'_k denoten les funcions simètriques elementals en les variables $X_1,\ldots,X_{n-1}$. Contradicció amb la hipòtesi d'inducció. □

El discriminant. L'expressió següent

$$\prod_{i<j}(X_i - X_j)^2$$

és un polinomi simètric en les variables $X_1,\ldots,X_n$ i, per tant, s'escriu com un polinomi en les funcions simètriques elementals d'aquestes variables.

Sigui $f(X)$ un polinomi en una variable,

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n = a_0(X-\alpha_1)\cdots(X-\alpha_n).$$

El *discriminant* del polinomi f és

$$\operatorname{disc} f = a_0^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Com que $\prod(\alpha_i - \alpha_j)^2$ té una expressió polinòmica en les funcions simètriques elementals de les arrels, $\operatorname{disc} f$ admet una expressió polinòmica en els coeficients $a_0,\ldots,a_n$.

En particular, si $A_0,\ldots,A_n$ són variables independents i $f(X)$ és el polinomi $A_0X^n + \cdots + A_n$ sobre l'anell $\mathbb{Z}[A_0,\ldots,A_n]$, obtenim un polinomi en les variables A_i

$$\operatorname{disc}(A_0,A_1,\ldots,A_n) \in \mathbb{Z}[A_0,\ldots,A_n]$$

que, en substituïr A_k pels coeficients d'un polinomi sobre un anell, dóna el discriminant d'aquest polinomi. Observem que a aquesta expresió ha desaparegut tota referència a les arrels del polinomi.

La resultant. L'expressió següent

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j)$$

és un polinomi simètric tant si el considerem com a polinomi en les variables $X_1,\ldots,X_n$ com si el considerem en les variables $Y_1,\ldots,Y_m$ i, per tant, s'escriu com un polinomi en $S_1,\ldots,S_n$ i $T_1,\ldots,T_m$, les funcions simètriques elementals respectives.

Siguin $f(X)$ i $g(X)$ polinomis en una variable,

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n = a_0(X-\alpha_1)\cdots(X-\alpha_n),$$

$$g(X) = b_0X^m + b_1X^{m-1} + \cdots + b_m = b_0(X-\beta_1)\cdots(X-\beta_m).$$

Es defineix la *resultant* $\mathrm{Res}(f,g)$ com

$$\mathrm{Res}(f,g) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Com que $\prod\prod(\alpha_i - \beta_j)$ té una expressió polinòmica en les funcions simètriques elementals de les arrels α_i i de les arrels β_j, $\mathrm{Res}(f,g)$ és un polinomi en $a_0,\ldots,a_n,b_0,\ldots,b_m$.

En particular, si $A_0,\ldots,A_n$ i $B_0,\ldots,B_m$ són variables i considerem els polinomis $f(X) = A_0X^n + A_1X^{n-1} + \cdots + A_n$ i $g(X) = B_0X^m + B_1X^{m-1} + \cdots + B_m$ com a polinomis sobre l'anell $\mathbb{Z}[a_0,\ldots,A_n,B_0,\ldots,B_m]$, obtenim un polinomi

$$\mathrm{Res}(A_0,\ldots,A_n,B_0,\ldots,B_m) \in \mathbb{Z}[A_0,\ldots,A_n,B_0,\ldots,B_m]$$

que, en substituir les A_k i les B_k pels coeficients de dos polinomis sobre un anell, s'obté la resultant d'aquests polinomis.

És important observar que tenim les expresions següents

$$\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_0^n \prod_{j=1}^{m} f(\beta_j).$$

Proposició 4.3. *Si $f(X)$ és un polinomi de grau n i primer coeficient a_0, aleshores*

$$\mathrm{Res}(f,f') = (-1)^{n(n-1)/2} a_0 \,\mathrm{disc}\, f.$$

PROVA: Les expressions a banda i banda de la igualtat s'obtenen avaluant els polinomis resultant i discriminant sobre els coeficients corresponents, per tant n'hi ha prou a comprovar la igualtat per al polinomi

$$f(X) = A_0X^n + A_1X^{n-1} + \cdots + A_n = A_0(X-X_1)\cdots(X-X_n).$$

Tenint en compte les propietats de la derivació,

$$f'(X) = A_0 \sum_{i=1}^{n}\prod_{j\neq i}(X - X_j)$$

i, per tant, $f'(X_i) = A_0\prod_{j\neq i}(X_i - X_j)$. Aleshores

$$\mathrm{Res}(f,f') = A_0^{n-1}\prod_{i=1}^{n} f'(X_i) = A_0^{2n-1}\prod_{i=1}^{n}\prod_{j\neq i}(X_i - X_j)$$

i, canviant de signe la meitat dels $n(n-1)$ factors,

$$(-1)^{n(n-1)/2} A_0^{2n-1} \prod_{i<j} (X_i - X_j)^2 = (-1)^{n(n-1)/2} A_0 \operatorname{disc} f.$$

□

5.– Mòduls i aplicacions lineals

Mòduls sobre un anell. Sigui R un anell (unitari, commutatiu). Un R-mòdul M és un grup abelià additiu amb una operació externa $R \times M \to M$ multiplicativa tal que

$$a(x+y) = ax + ay, \quad a(bx) = (ab)x, \quad 1x = x.$$

Donar una estructura de R-mòdul a un grup abelià M equival a donar un homomorfisme d'anells $R \to \operatorname{End} M$ de l'anell R en l'anell d'endomorfismes de M com a grup abelià.

Per exemple, tot ideal de l'anell R és un R-mòdul, tot quocient de R per un ideal és un R-mòdul, els anells de polinomis $R[X]$ i $R[X_1, \ldots, X_n]$ són R-mòduls, tot anell que contingui R com a subanell és un R-mòdul, tot grup abelià és un $\mathbb{Z}$-mòdul, els espais vectorials són els mòduls sobre un cos.

Es definexien de la manera habitual submòdul, mòdul quocient, homomorfisme. Un homomorfisme de R-mòduls s'anomena també aplicació *lineal* (o R-lineal).

El producte directe d'una família $\{M_i\}_{i \in I}$ de R-mòduls és el producte cartesià amb les operacions component a component. Es denota $\prod_{i \in I} M_i$. La suma directa (externa) és el submòdul format pels elements del producte directe que tenen quasi totes les coordenades zero. Es denota $\bigoplus_{i \in I} M_i$.

Siguin $\{M_i\}_{i \in I}$ submòduls d'un R-mòdul M. La seva *suma* $\sum_{i \in I} M_i$ és el submòdul més petit de M que els conté tots i està format per les sumes finites $x_{i_1} + \cdots + x_{i_n}$ amb $x_{i_j} \in M_{i_j}$. La suma s'anomena *suma directa* (interna) quan $M_i \cap (\sum_{j \neq i} M_j) = 0$ per tot i; o sigui, quan l'expressió de cada element com a suma d'elements dels M_i és única. Quan la suma és directa es denota $\bigoplus_{i \in I} M_i$.

Mòduls lliures. Sigui $\{x_i\}_{i \in I}$ una família d'elements d'un R-mòdul M. Una *combinació lineal* dels x_i és una suma finita

$$a_1 x_{i_1} + a_2 x_{i_2} + \cdots + a_n x_{i_n}, \qquad a_j \in R.$$

Els a_j són els *coeficients* de la combinació lineal. Les combinacions lineals dels x_i formen un submòdul $N \subseteq M$. És el més petit que conté tots aquests elements; o sigui, el submòdul

generat pel conjunt $\{x_i\}_{i\in I}$. Un R-mòdul és *finitament generat* si admet una família finita de generadors, i *cíclic* si es pot generar amb un sol element: $M = Ax$.

Els x_i són *linealment independents* si l'única combinació lineal igual a zero és la que té tots els coeficients iguals a zero. És a dir, els x_i són linealment independents si cada element del mòdul generat per $\{x_i\}$ s'escriu com a combinació lineal dels x_i de manera única.

Una *base* d'un R-mòdul M és un subconjunt independent que el genera. No tot R-mòdul té una base; per exemple, $\mathbb{Z}_n$ i $\mathbb{Q}$ no tenen cap base com a $\mathbb{Z}$-mòduls. Un R-mòdul *lliure* és un que té alguna base. Tot espai vectorial és lliure.

Si I és un conjunt d'índexos, denotem $\bigoplus_{i\in I} R$ la suma directa externa de tants mòduls isomorfs a R com el cardinal de I. Quan I és finit, de cardinal n, el denotem R^n. Aquest és un mòdul lliure amb una base formada pels elements que tenen totes les coordenades iguals a zero llevat d'una, que és 1.

Si M és un mòdul lliure amb base $\{x_i\}_{i\in I}$ i N és un mòdul qualsevol, tota aplicació $\{x_i\} \to N$ s'extén de manera única a una aplicació lineal $M \to N$. Aquesta propietat caracteritza les bases d'un mòdul.

Aplicacions lineals i matrius. Siguin $X = \{x_1, \ldots, x_m\}$ i $Y = \{y_1, \ldots, y_n\}$ bases dels R-mòduls lliures M i N. A cada aplicació lineal $f\colon M \to N$ li associem la matriu $\mathrm{Mat}(f, X, Y) = (a_i^j) \in M_{n\times m}(R)$ amb coeficients determinats per $f(x_j) = \sum_{i=1}^n a_{ij} y_i$. Les columnes de $\mathrm{Mat}(f, X, Y)$ són les coordenades dels vectors $f(x_j)$ en la base Y.

Si $g\colon N \to N_1$ és una altra aplicació lineal i N_1 és lliure amb base Z, aleshores $\mathrm{Mat}(gf, X, Z) = \mathrm{Mat}(g, Y, Z)\,\mathrm{Mat}(f, X, Y)$. O sigui, a la composició d'aplicacions lineals li correspon el producte de matrius.

Recíprocament, si $A \in M_{n\times m}(R)$ és una matriu qualsevol, l'aplicació lineal determinada per $f(x_j) = \sum_{i=1}^n a_i^j y_j$ té matriu $\mathrm{Mat}(f, X, Y) = A$.

Determinants. El *determinant* d'una matriu quadrada $A = \{a_i^j\} \in \mathrm{M}_n(R)$ és

$$\det A = \sum_{\sigma\in\mathfrak{S}_n} \operatorname{sgn}\sigma \prod_{i=1}^n a^i_{\sigma(i)}.$$

Manipulant aquesta expressió es comproven les propietats del determinant:

- és lineal respecte cada columna (fila);
- si dues columnes (files) són iguals, val zero;
- en permutar les columnes (files) queda multiplicat pel signe de la permutació;
- en sumar a una columna (fila) una combinació lineal de les demés no canvia;
- $\det A^t = \det A$;
- $\det AB = \det A \det B$.

L'*adjunt* (i, j)-èsim de la matriu A és el determinant de la matriu de $M_{n-1}(R)$ que resulta en suprimir la fila i-èsima i la columna j-èsima de la matriu A, afectat del signe $(-1)^{i+j}$.

Anomenem-lo A_i^j. La fórmula següent es coneix com a *regla de Laplace:*

$$\sum_{k=1}^{n} a_k^i A_k^j = \begin{cases} \det A, & i = j, \\ 0, & i \neq j. \end{cases}$$

D'aquí es dedueix immediatament que, si $A^* = \{A_i^j\}$ és la *matriu adjunta* de la matriu A, $A(A^*)^t = (\det A)I_n$, on I_n és la matriu identitat $n \times n$. D'aquesta expressió i de la multiplicativitat dels determinants en resulta que A és invertible a $\mathrm{M}_n(R)$ si, i només si, $\det A \in R^*$ i, en aquest cas, $A^{-1} = (\det A)^{-1}(A^*)^t$.

Proposició 5.1. *Si $A \in M_{n\times m}(R)$ i $B \in M_{m\times n}(R)$, aleshores $AB \in M_n(R)$. Si $n > m$, $\det AB = 0$. Si $n \leqslant m$, per cada subconjunt $S = \{i_1, i_2, \ldots, i_n\} \subseteq \{1, 2, \ldots, m\}$ sigui A^S la submatriu quadrada de A formada per les columnes $i_1, \ldots, i_n$ i B_S la submatriu quadrada de B formada per les files $i_1, \ldots, i_n$. Aleshores $\det AB = \sum_S \det A^S \det B_S$.*

PROVA: Si $n > m$, sigui A_1 la matriu obtinguda afegint $m - n$ columnes de zeros al final de A i B_1 la matriu obtinguda afegint $m - n$ files de zeros al final de B. Aleshores $A_1B_1 = AB$. Per tant, $\det AB = \det A_1 \det B_1 = 0$.

El cas $n \leqslant m$ és una generalització de la multiplicativitat del determinant (que és el cas $n = m$) i es demostra exactament igual. Escrivim $A = (a^1, \ldots, a^m)$ i $B = (b^1, \ldots, b^n)$, on a^i i b^j són les columnes respectives. Aleshores

$$AB = (Ab^1, \ldots, Ab^n) = (\sum_{k=1}^{m} a^k b_k^1, \ldots, \sum_{k=1}^{m} a^k b_k^n),$$

i, per linealitat respecte les columnes,

$$\det AB = \sum_{k_1=1}^{m} \cdots \sum_{k_n=1}^{m} b_{k_1}^1 \cdots b_{k_n}^n \det(a^{k_1}, \ldots, a^{k_n}).$$

Com que si hi ha dues columnes iguals el determinant val zero, del sumatori només sobreviuen els sumands amb els k_i tots diferents. Per cada subconjunt $S = \{i_1, \ldots, i_n\} \subseteq \{1, \ldots, m\}$ tindrem un sumand per cada permutació dels i_j, o sigui,

$$\det AB = \sum_S \sum_{\sigma \in \mathfrak{S}_n} b_{\sigma(i_1)}^1 \cdots b_{\sigma(i_n)}^n \det(a^{\sigma(i_1)}, \cdots, a^{\sigma(i_n)}),$$

i, tenint en compte que en permutar les columnes d'una matriu el determinant queda afectat del signe de la permutació,

$$\det AB = \sum_S \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}\sigma \; b_{\sigma(i_1)}^1 \cdots b_{\sigma(i_n)}^n \det(a^{i_1}, \cdots, a^{i_n}),$$

que, treient factor comu dels $\det A^S$, és $\sum_S \det A^S \det B_S$. □

Teorema 5.2. *Sigui $R \neq 0$. Totes les bases d'un R-mòdul lliure tenen el mateix cardinal, que s'anomena dimensió del mòdul. En particular, $R^m \simeq R^n \Rightarrow m = n$.*

PROVA: Només per al cas finit. Suposem que M té una base finita $X = \{x_1, \ldots, x_n\}$. Qualsevol altra base $\{y_i\}$ ha de ser finita, ja que cada x_i és combinació lineal d'un nombre finit de y_j i, per tant, amb un nombre finit de y_j n'hi ha prou per generar M.

Sigui, doncs, $Y = \{y_1, \ldots, y_m\}$ una altra base de M. Siguin $A = \mathrm{Mat}(Id, X, Y) \in M_{m\times n}(R)$ i $B = \mathrm{Mat}(Id, Y, X) \in M_{n\times m}(R)$ les matrius de l'aplicació identitat $Id\colon M \to M$ en aquestes bases. Aleshores $AB = I_m$ i $BA = I_n$. Per la proposició anterior, si $n < m$ aleshores $0 = \det AB = \det I_m = 1$ i si $n > m$ aleshores $0 = \det BA = \det I_n = 1$. Per tant, necessàriament $n = m$. □

Canvis de base. A un R-mòdul lliure de dimensió finita totes les bases tenen el mateix cardinal, i la matriu de l'aplicació identitat $Id\colon M \to M$, calculada en bases diferents, proporciona una matriu invertible; recíprocament, tota matriu invertible és la matriu d'aquesta aplicació en certes bases.

Es denota $\mathrm{GL}_n(R)$ el grup multiplicatiu de les matrius invertibles. Està format per matrius de $\mathrm{M}_n(R)$ amb determinant invertible a R. També es pot caracteritzar com el conjunt de totes les matrius que representen l'aplicació identitat a un R-mòdul lliure de dimensió n.

Siguin M i N mòduls lliures de dimensions m i n amb bases X i Y respectivament. Si $f\colon M \to N$ és una aplicació lineal, considerem la matriu $A = \mathrm{Mat}(f, X, Y)$. Si X' i Y' són unes altres bases de M i N,

$$B = \mathrm{Mat}(f, X', Y') = \mathrm{Mat}(Id, Y, Y')\,\mathrm{Mat}(f, X, Y)\,\mathrm{Mat}(Id, X', X),$$

de manera que $B = PAQ$ amb $P \in \mathrm{GL}_n(R)$ i $Q \in \mathrm{GL}_m(R)$. Recíprocament, per qualsevol parell de matrius P i Q com les indicades, la matriu PAQ és la matriu de l'aplicació lineal f corresponent a certes bases de M i N. Dues matrius $A, B \in \mathrm{M}_{n\times m}(R)$ en aquestes condicions s'anomenen *equivalents*.

Si $f\colon M \to M$ és un endomorfisme, i X és una base de M, sigui $A = \mathrm{Mat}(f, X)$ la matriu de l'endomorfisme calculada en la base X. Si X' és una altra base,

$$B = \mathrm{Mat}(f, X') = \mathrm{Mat}(Id, X', X)^{-1}\,\mathrm{Mat}(f, X)\,\mathrm{Mat}(Id, X', X),$$

de manera que $B = P^{-1}AP$ amb $P \in \mathrm{GL}_m(R)$. Recíprocament, per cada matriu $P \in \mathrm{GL}_m(R)$ la matriu $P^{-1}AP$ és la matriu de l'endomorfisme f corresponent a alguna base de M. Dues matrius $A, B \in \mathrm{M}_m(R)$ en aquestes condicions s'anomenen *semblants*.

Transformacions elementals. Certs canvis de base s'anomenen *transformacions elementals*. Concretament:

- canviar d'ordre els elements d'una base;
- multiplicar cada element d'una base per un invertible de l'anell;
- sumar a un element de la base una combinació lineal d'un altre.

Les matrius que els corresponen (*matrius elementals*) són:

- *matrius de permutació*: la matriu identitat amb les columnes permutades. Formen un subgrup de $\mathrm{GL}_m(R)$ isomorf al simètric $\mathfrak{S}_m$.
- Les matrius diagonals invertibles. Formen un subgrup de $\mathrm{GL}_m(R)$ isomorf a $(R^*)^m$.
- Les matrius que tenen coeficients 1 a la diagonal i termes no nuls només a una columna o fila (transveccions).

L'efecte que té sobre la matriu d'una aplicació lineal $f\colon M \to N$ el fer un canvi de base dels tipus anteriors al mòdul M és:

- canviar d'ordre les columnes;
- multiplicar les columnes per invertibles de l'anell;
- sumar a una columna una combinació lineal de les altres;

respectivament. Si R és un cos, tot canvi de base s'obté a partir d'un nombre finit de transformacions elementals. Per tant, les matrius elementals generen el grup $\mathrm{GL}_m(R)$. A un anell commutatiu, en general això no és així.

Ideals de Fitting. Sigui $A \in \mathrm{M}_{n\times m}(R)$ una matriu sobre un anell R. Sigui $t = \min(n, m)$. Si $1 \leqslant k \leqslant t$, el k-èsim *ideal de Fitting* (o *ideal determinantal*) de la matriu A és l'ideal generat per tots els seus menors d'ordre k. El denotem $\mathfrak{a}_k(A)$. De la regla de Laplace es dedueix immediatament que

$$\mathfrak{a}_1(A) \supseteq \mathfrak{a}_2(A) \supseteq \cdots \supseteq \mathfrak{a}_t(A).$$

En particular, una matriu quadrada és invertible si, i només si, tots els seus ideals de Fitting són iguals a R.

Si $AQ = B$, tota submatriu $k \times k$ de B és el producte de k files de A per k columnes de Q i, per la proposició 5.1, $\mathfrak{a}_k(B) \subseteq \mathfrak{a}_k(A)\mathfrak{a}_k(Q)$. En particular, si $Q \in \mathrm{GL}_m(R)$ aleshores $\mathfrak{a}_k(A) = \mathfrak{a}_k(B)$, i els ideals de Fitting són invariants de la classe d'equivalència.

En cas que R sigui un cos, tots els ideals de Fitting són (1) ó 0. El més gran $1 \leqslant r \leqslant t$ tal que $\mathfrak{a}_r(A) = (1)$ és el *rang* de la matriu.

6.– Mòduls sobre DIP

Mòduls sobre anells íntegres. Torsió. Suposem que R és un anell íntegre i M és un R-mòdul. Un element $x \in M$ és *de torsió* si existeix un $a \neq 0$ amb $ax = 0$. Els elements de torsió formen un submòdul de M, que denotarem M_{tors}. El mòdul M és *de torsió* quan $M = M_{\mathrm{tors}}$ i és *lliure de torsió* quan $M_{\mathrm{tors}} = 0$. Un mòdul cíclic no trivial Rx és lliure si, i només si, l'element x no és de torsió. Un mòdul és lliure si, i només si, és lliure de torsió i és suma directa de mòduls cíclics no trivials.

Teorema 6.1. (*Forma normal de Smith*). *Tota matriu $A \in M_{n\times m}(R)$ sobre un DIP és equivalent a una matriu de la forma*

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \\ & & \end{pmatrix},$$

on $d_1, \ldots, d_r$ són elements no nuls de R tals que $d_i \mid d_{i+1}$. A més, la matriu A determina completament els d_i llevat d'unitats. Una matriu d'aquestes característiques s'anomena en forma normal de Smith. Els d_i són els divisors elementals de la matriu A.

PROVA: Si $a, b \in A$ amb $a \neq 0$, sigui $(d) = (a, b)$ el seu màxim comú divisor. Existeixen elements $x, y \in A$ tals que $ax + by = d$. Aleshores es tenen les identitats matricials

$$\begin{pmatrix} a & b & \cdots \\ \ddots & \ddots & \end{pmatrix} \begin{pmatrix} x & -b/d & \\ y & a/d & \\ & & I_{m-2} \end{pmatrix} = \begin{pmatrix} d & 0 & \cdots \\ \ddots & \ddots & \end{pmatrix},$$

$$\begin{pmatrix} x & y & \\ -b/d & a/d & \\ & & I_{n-2} \end{pmatrix} \begin{pmatrix} a & \ddots \\ b & \\ \vdots & \ddots \end{pmatrix} = \begin{pmatrix} d & \ddots \\ 0 & \\ \vdots & \ddots \end{pmatrix}.$$

Aquestes identitats corresponen a certs canvis de base, que anomenarem transformacions de tipus I i tipus II, respectivament. Per demostrar el teorema donarem un procediment que, en un nombre finit de passos, permet convertir la matriu donada en una matriu en forma normal de Smith fent transformacions elementals i transformacions del tipus I i II. Per assegurar la finitud de l'algoritme convé recordar que a un DIP un element no nul només té un nombre finit de divisors (llevat unitats). Les transformacions de tipus I i II, en el cas que $a \nmid b$, canvien a per un divisor estricte.

Si $A = 0$, A ja està en forma normal. En cas contrari, permutant files i columnes si cal, podem aconseguir que $a_1^1 \neq 0$. Aleshores:

(1) Per cada $j = 2, \ldots, m$, mentre $a_1^1 \mid a_1^j$, restem a la columna j-èsima un multiple adequat de la primera de manera que quedi $a_1^j = 0$. Si $a_1^1 \nmid a_1^j$, intercanviem les columnes segona i j-èsima, apliquem una transformació de tipus I, i tornem a començar. Després d'un nombre finit de passos aconseguirem que $a_1^j = 0$ per tot $j = 2, \ldots, m$.

(2) Per cada $i = 2, \ldots, n$, mentre $a_1^1 \mid a_i^1$, restem a la fila i-èsima un multiple adequat de la primera de manera que quedi $a_i^1 = 0$. Si $a_1^1 \nmid a_i^1$, intercanviem les files segona i i-èsima, apliquem una transformació de tipus II, i tornem a començar. Després d'un nombre finit de passos aconseguirem que $a_i^1 = 0$ per tot $i = 2, \ldots, n$.

Fent alternativament (1) i (2) un nombre finit de vegades arribarem a una matriu del tipus

$$\begin{pmatrix} a_1^1 & 0 & 0 \\ 0 & & \\ & A_1 & \\ 0 & & \end{pmatrix}.$$

Aleshores, per cada $i > 1$ i $j > 1$, si $a_1^1 \nmid a_i^j$ sumem la fila i-èsima a la primera, intercanviem les columnes segona i j-èsima, apliquem una transformació de tipus I i tornem a començar per (1). Repetint aquest procés mentre sigui necessari, despres d'un nombre finit de passos arribarem a una matriu del tipus

$$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & & \\ & A_1 & \\ 0 & & \end{pmatrix},$$

amb $d_1 \mid a_i^j$ per tot i, j. Fent el mateix amb la submatriu A_1, i tenint en compte que els seus termes es divideixen tots per d_1, aribarem a una del tipus

$$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & \\ & & A_2 \\ 0 & & \end{pmatrix}.$$

amb $d_1 \mid d_2$ i d_2 dividint tots els coeficients de la matriu A_2. Reiterant les vegades necessàries arribarem a la forma normal de Smith.

La unicitat prové del fet que els ideals de Fitting són invariants de les classes d'equivalència de matrius,

$$\mathfrak{a}_1(A) = (d_1), \quad \mathfrak{a}_2(A) = (d_1 d_2), \ldots, \quad \mathfrak{a}_r(A) = (d_1 \cdots d_r), \qquad \mathfrak{a}_k = 0,\ k > r,$$

i els d_i queden determinats, llevat d'unitats, pel fet que d_1 és un generador de $\mathfrak{a}_1(A)$ i els altres d_i són el quocient entre un generador de $\mathfrak{a}_{i+1}(A)$ i un de $\mathfrak{a}_i(A)$. □

Teorema 6.2. *Sigui R un DIP. Tot submòdul d'un R-mòdul lliure és lliure, de dimensió menor o igual que la del mòdul.*

PROVA: Només per dimensió finita. Sigui M un R-mòdul lliure amb base $\{x_1, \ldots, x_m\}$ i N un submòdul. Per cada $1 \leqslant r \leqslant m$ sigui N_r la intersecció de N amb el submòdul generat per $x_1, \ldots, x_r$ i prenem $N_0 = 0$. Demostrarem per inducció que cada N_r és lliure de dimensió $\leqslant r$. $N_0 = 0$ és lliure de dimensió zero; suposem-ho comprovat fins a $r - 1$. Sigui

$$\mathfrak{a} = \{\, a_k \in R \mid \exists x \in N_r,\ x = a_1 x_1 + \cdots + a_k x_k \,\}.$$

És clar que $\mathfrak{a}$ és un ideal de R. Si $\mathfrak{a} = 0$, $N_r = N_{r-1}$ i ja hem acabat. Si $\mathfrak{a} \neq 0$, sigui $a \neq 0$ un generador, i sigui $x \in N_r$ un element de la forma $x = b_1 x_1 + \cdots + b_{r-1} x_{r-1} + a x_r$. Aleshores $N_r = N_{r-1} \oplus Rx$. En efecte, la inclusió $N_{r-1} + Rx \subseteq N_r$ és evident. Si $y = b_1 x_1 + \cdots + b_r x_r \in N_r$, sigui $b_r = ca$; aleshores $y - cx \in N_{r-1}$, per tant tenim la inclusió contraria. El fet que la suma és directa és clar: un element de Rx que tingui coeficient de x_r igual a zero ha de ser zero. Per hipòtesi d'inducció, N_{r-1} és una suma directa de $r - 1$ o menys R-mòduls ciclics. Per tant, N_r és suma directa de r o menys mòduls cíclics. Com que és lliure de torsió, és lliure de dimensió $\leqslant r$. □

Teorema 6.3. (*Classificació dels mòduls finitament generats sobre DIP*). *Sigui R un DIP. Tot R-mòdul finitament generat és isomorf a un producte*

$$R/(d_1) \times \cdots \times R/(d_t) \times R^r,$$

on els $d_i \in R$ són elements no nuls, no unitats, amb $d_i \mid d_{i+1}$. Aquesta descomposició és única, en el sentit que els nombres r i t i els ideals (d_i) queden completament determinats pel mòdul donat.

PROVA: Suposem que el mòdul M està generat per n elements. Sigui E un mòdul lliure de dimensió n i $E \to M$ l'epimorfisme que envia cada element d'una base de E a un dels generadors de M. Sigui F el nucli d'aquest epimorfisme, que és un mòdul lliure de dimensió $n \leqslant m$. Siguin $X = \{x_1, \ldots, x_n\}$ i $Y = \{y_1, \ldots, y_m\}$ bases de F i E en les quals la matriu de la inclusió $F \to E$ està en forma normal de Smith, i siguin $d_1, \ldots, d_n$ els divisors elementals corresponents (n'hi ha n perquè la inclusió és injectiva). Aleshores $x_i = d_i y_i$ per tot $i = 1, \ldots, n$ i

$$M \simeq E/F = \frac{Ry_1 \oplus \cdots \oplus Ry_n \oplus \cdots \oplus Ry_m}{Rx_1 \oplus \cdots \oplus Rx_n} \simeq R/(d_1) \times \cdots \times R/(d_n) \times R^{m-n}.$$

Eliminant els factors trivials, corresponents als d_i que són unitats, obtenim una descomposició com la demanada.

Per comprovar la unicitat, considerem $M \simeq R/(e_1) \times \cdots \times R/(e_u) \times R^s$ una altra descomposició de les mateixes característiques. Aleshores $R^r \simeq (d_t e_u)M \simeq R^s \Rightarrow t = s$ i

$$R/(d_1) \times \cdots \times R/(d_t) \simeq M_{\text{tors}} \simeq R/(e_1) \times \cdots \times R/(e_u).$$

Per tant, ens podem restringir al cas que M és de torsió. Suposem que tenim dos productes de mòduls cíclics de torsió isomorfs, segons les notacions anteriors. Demostrarem la igualtat dels ideals (d_i) i (e_j) per inducció sobre el nombre de factors primers que divideixen d_t. Observem que si p és un primer de R i a un element qualsevol,

$$(p)R/(a) = \begin{cases} R/(a), & p \nmid a, \\ (p)/(a) \simeq R/(a/p), & p \mid a, \end{cases} \qquad \frac{R/(a)}{(p)R/(a)} \simeq \begin{cases} 0, & p \nmid a, \\ R/(p), & p \mid a. \end{cases}$$

Sigui p un primer que divideix d_1. Suposem que p no divideix $e_1, \ldots, e_k$ i que divideix $e_{k+1}, \ldots, e_u$, amb $0 \leqslant k \leqslant u$. Aleshores,

$$\prod_{i=1}^{t} R/(p) \simeq \prod_{i=1}^{t} \frac{R/(d_i)}{(p)R/(d_i)} \simeq M/(p)M \simeq \prod_{j=1}^{u} \frac{R/(e_j)}{(p)R/(e_j)} \simeq \prod_{j=k+1}^{u} R/(p).$$

Per tant, $t = u - k \leqslant u$. El mateix argument, amb un primer que divideixi e_1, permet demostrar la desigualtat contraria. Per tant, $t = u$ i $p \mid d_1 \Leftrightarrow p \mid e_1$.

Sigui $p \mid d_1$ i siguin $d_i' = d_i/p$, $e_i' = e_i/p$. Aleshores,

$$R/(d_1') \times \cdots \times R/(d_n') \simeq (p)M \simeq R/(e_1') \times \cdots \times R/(e_n').$$

A cada costat pot haver-hi factors trivials, corresponents als d_i i als e_i iguals a p. Eliminant aquests possibles factors, i tenint en compte que d_n' té un factor primer menys que d_n, per hipòtesi d'inducció $(d_i') = (e_i')$ i, per tant, $(d_i) = (e_i)$. □

Corol·lari 6.4. (*Classificació dels grups abelians finitament generats*). *Tot grup abelià finitament generat és isomorf a un producte*

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_t} \times \mathbb{Z}^r.$$

amb d_i enters, $d_i > 1$, $d_i \mid d_{i+1}$, univocament determinats.

Endomorfismes d'un espai vectorial. Sigui K un cos, V un K-espai vectorial de dimensió finita n, i $\phi \in \mathrm{End}_K(V)$ una aplicació lineal $V \to V$. Sigui $R = K[X]$ l'anell de polinomis en una variable. Hi ha un (únic) homomorfisme d'anells $K[X] \to \mathrm{End}_K(V)$ que envia les constants a les homotècies i X a ϕ. Denotem $f(\phi)$ la imatge d'un polinomi $f(X)$ per aquest homomorfisme. Definim una estructura de R-mòdul a V amb el producte

$$f(X)v = f(\phi)v.$$

Aquesta estructura és compatible amb la d'espai vectorial en el sentit que pensem els elements $a \in K$ com a polinomis constants, el producte av és el mateix considerant V com a K-espai vectorial que considerant-lo com a R-mòdul. Per distingir-los, denotarem V_ϕ l'espai V amb l'estructura de R-mòdul.

Si $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$ és un polinomi mònic, la seva *matriu companya* és la matriu

$$A_f = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & 0 & & -a_2 \\ \vdots & & & 0 & \vdots \\ 0 & 0 & & 1 & -a_{n-1} \end{pmatrix}.$$

Teorema 6.5. (*Classificació d'endomorfismes*). *Sigui K un cos, V un K-espai vectorial de dimensió finita, $\phi \in \mathrm{End}_K(V)$ un endomorfisme, $R = K[X]$, i V_ϕ l'espai V amb l'estructura de R-mòdul corresponent a l'endomorfisme ϕ. Aleshores:*

(a) *V_ϕ és finitament generat i de torsió com a R-mòdul.*

(b) *Existeixen polinomis mònics no constants $d_i(X)$, amb $d_i \mid d_{i+1}$, tals que*

$$V_\phi \simeq R/(d_1(X)) \times \cdots \times R/(d_r(X)).$$

Aquests polinomis queden unívocament determinats per ϕ i s'anomenen els divisors elementals de l'endomorfisme.

(c) *Dos endomorfismes tenen els mateixos divisors elementals si, i només si, són conjugats.*

(d) *Existeix una K-base de V en què la matriu de ϕ és la suma directa de les matrius companyes dels $d_i(X)$,*

$$\begin{pmatrix} A_{d_1} & & \\ & \ddots & \\ & & A_{d_r} \end{pmatrix}.$$

Una matriu com aquesta s'anomena en forma racional.

(e) *Si $A \in M_n(K)$ és la matriu de l'endomorfisme en una base qualsevol, els divisors elementals de l'endomorfisme són els de la matriu $XI_n - A \in M_n(R)$.*

(f) *El polinomi característic* $\det(XI_n - A)$ *s'anul·la a ϕ (teorema de Cayley-Hamilton).*

PROVA: (a) Qualsevol K-base de l'espai genera V_ϕ sobre R. Si $v \in V$, els $n+1$ vectors $v, \phi(v), \phi^2(v), \ldots, \phi^n(v)$ no poden ser K-independents, per tant existeixen $a_0, \ldots, a_n \in K$ no tots nuls amb $a_0v + a_1\phi(v) + \cdots + a_n\phi^n(v) = 0$. Aleshores $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ és un polinomi no nul tal que $f(X)v = 0$.

(b) És el teorema de classificació de mòduls finitament generats sobre DIP aplicat al mòdul V_ϕ sobre l'anell R.

(c) Pel teorema de classificació de mòduls finitament generats sobre DIP, els endomorfismes ϕ i ψ tenen els mateixos divisors elementals si, i només si, $V_\phi \simeq V_\psi$ com a R-mòduls. Un isomorfisme de R-mòduls és, en particular, un isomorfisme de K-espais vectorials. Si $\sigma\colon V_\phi \to V_\psi$ és un isomorfisme de K-espais vectorials, la condició per tal que sigui isomorfisme de R-mòduls és que $X\sigma(v) = \sigma(Xv)$ per tot v. Tenint en compte les dues estructures, això equival a què $\psi\sigma(v) = \sigma\phi(v)$ per tot v; o sigui, a què $\phi = \sigma^{-1}\psi\sigma$ com a aplicacions K-lineals.

(d) Siguin $d_1(X), \ldots, d_r(X)$ els divisors elementals de ϕ. Sigui $V_\phi = Rv_1 \oplus \cdots \oplus Rv_r$ la descomposició en suma directa corresponent a la descomposició del teorema d'estructura. Els v_i són vectors amb $f(X)v_i = 0 \Leftrightarrow d_i(X) \mid f(X)$. Siguin $n_1, \ldots, n_r$ els graus dels divisors elementals. Tot element $v \in V$ s'escriu com $v = f_1(X)v_1 + \cdots + f_r(X)v_r$, on cada $f_i(X)$ es pot suposar, fent divisió euclidiana per $d_i(X)$, de grau menor que n_i. Per tant, tot vector és una combinació lineal sobre K dels vectors

$$v_1, \phi(v_1), \ldots, \phi^{n_1-1}(v_1), \ldots\ldots, v_r, \phi(v_r), \ldots, \phi^{n_r-1}(v_r).$$

Una combinació lineal trivial d'aquests vectors amb coeficients a K porporciona una igualtat $\sum f_i(X)v_i = 0$, amb polinomis $f_i(X)$ de graus menors que n_i. Com que la suma és directa, cada $f_i(X)v_i$ ha de ser zero. Per tant, $d_i(X) \mid f_i(X)$ i, tenint en compte els graus, $f_i(X) = 0$. Això demostra la independència dels vectors considerats. La matriu de ϕ en aquesta base és la matriu que té per caixes les matrius companyes dels divisors elementals.

(e) Diguem $A = (a_i^j)$, de manera que $\phi(v_j) = \sum_{i=1}^n a_i^j v_i$. Els vectors v_i generen V_ϕ com a R-mòdul. Sigui E un R-mòdul lliure de dimensió n amb base $\{x_1, \ldots, x_n\}$, i considerem l'epimorfisme de R-mòduls $E \to V_\phi$ que envia cada x_i al vector v_i. Sigui F el nucli d'aquest epimorfisme. Aleshores F admet com a base els elements

$$y_j = Xx_j - \sum_{i=1}^n a_i^j x_i, \quad 1 \leqslant j \leqslant n.$$

En efecte, és clar que aquests elements són de F. Sigui $x = f_1(X)x_1 + \cdots + f_n(X)x_n \in E$ un element qualsevol. Utilitzant recursivament les fórmules

$$Xx_j = y_j + \sum_{i=1}^n a_i^j x_i, \quad 1 \leqslant j \leqslant n,$$

podrem expressar x de la forma

$$x = g_1(X)y_1 + \cdots + g_n(X)y_n + \alpha_1 x_1 + \cdots + \alpha_n x_n,$$

on els $g_i(X)$ són polinomis (de grau menor que el màxim dels graus dels f_i), i els α_i són elements de K. Aleshores $x \in F \Leftrightarrow \alpha_1 v_1 + \cdots + \alpha_n v_n = 0 \Leftrightarrow \alpha_i = 0$ per tot i. Per tant, F està generat pels y_i.

D'altra banda, una combinació $\sum g_i(X)y_i = 0$ proporciona, substituïnt les y_i per la seva expressió en termes de les x_i, una combinació $\sum f_i(X)x_i = 0$. Si $g_j(X)$ té grau màxim entre els g_i aleshores $\deg f_j = \deg g_j + 1$. Per tant els y_i són R-independents.

Tenint en compte la demostració del teorema de classificació, els divisors elementals de ϕ són els de la matriu de la inclusió $F \to E$, que és la matriu $XI_n - A \in M_n(R)$.

(g) El polinomi característic $\det(XI_n - A)$ és el producte dels divisors elementals de la matriu $XI_n - A$. Per tant, s'anul·la a ϕ. □

Corol·lari 6.6. *Sigui K un cos i $R = K[X]$. Aleshores:*

(a) *Dues matrius $A, B \in M_n(K)$ són semblants sobre K si, i només si, les matrius $XI_n - A$ i $XI_n - B$ són equivalents sobre R.*

(b) *Dues matrius $A, B \in M_n(K)$ són semblants si, i només si, tenem la mateixa forma racional.*

PROVA: (a) Si A i B són semblants, representen un mateix endomorfisme en bases diferents. Per l'apartat (e) del teorema anterior, els divisors elementals de $XI_n - A$ i $XI_n - B$ són els d'aquest endomorfisme. Per tant aquestes matrius tenen els mateixos divisors elementals i són equivalents.

Suposem que $XI_n - A$ i $XI_n - B$ són equivalents. Siguin ϕ i ψ endomorfismes d'un K-espai vectorial de dimensió n que, en una certa base, tinguin per matriu A i B, respectivament. Els divisors elementals d'aquests endomorfismes són els mateixos i, per l'apartat (c) del teorema anterior, són conjugats $\psi = \sigma^{-1}\phi\sigma$. La matriu de σ en la base considerada conjuga A i B.

(b) Naturalment, entenem per *forma racional* d'una matriu A una matriu semblant que estigui en forma racional. El resultat es dedueix immediatament de l'apartat anterior. □

Tema III: COSSOS. TEORIA DE GALOIS

1.– Preliminars sobre cossos

Cossos. Un *cos* K és un anell commutatiu unitari, amb $1 \neq 0$, on tot element no nul té invers pel producte. Els elements no nuls de K són un grup amb el producte, que s'anomena *grup multiplicatiu* de K i es denota K^*.

Els únics ideals de K són el trivial i el total; per tant, tot homomorfisme de K en un anell unitari és injectiu. Els homomorfismes de cossos, necessariament injectius, s'anomenen també *immersions*. Es fa servir sovint la notació exponencial: $\sigma(a)$ es denota a^σ i la imatge de la immersió $\sigma\colon K \to L$ és el cos K^σ, subcos de L. Cal anar amb compte ja que amb la notació habitual les aplicacions operen per l'esquerra i amb la notació exponencial ho fan per la dreta. Per tant, cal definir $(\alpha^\sigma)^\tau = \alpha^{\tau\sigma}$.

Un homomorfisme de cossos $\sigma\colon K \to L$ indueix un homomorfisme entre els anells de polinomis corresponents $K[X] \to L[X]$ que consisteix en aplicar σ als coeficients dels polinomis, $f(X) = \sum a_i X^i \mapsto f^\sigma(X) = \sum a_i^\sigma X^i$. Aquest homomorfisme d'anells és injectiu i proporciona un isomorfisme de $K[X]$ en $K^\sigma[X]$. A cada factorització $f(X) = \sum g_i(X)^{m_i}$ a $K[X]$ li correspon la factorització $f^\sigma(X) = \sum g_i^\sigma(X)^{m_i}$ a $L[X]$. Si $f^\sigma(X)$ és irreductible a $L[X]$, $f(X)$ és irreductible a $K[X]$, però el recíproc no és cert; si $f(X)$ és irreductible a $K[X]$ l'únic que podem assegurar és que $f^\sigma(X)$ ho és a $K^\sigma[X]$, però pot tenir factoritzacions no trivials a $L[X]$. Si α és una arrel de multiplicitat m de $f(X)$, aleshores α^σ és una arrel de multiplicitat m de $f^\sigma(X)$.

Cos primer. Característica. El *cos primer* d'un cos K és el més petit subcos de K. Considerem l'únic homomorfisme d'anells $f\colon \mathbb{Z} \to K$, determinat pel fet que la imatge de $1 \in \mathbb{Z}$ és $1 \in K$. $\operatorname{Im} f$ és el més petit subanell contingut a K, i el cos primer de K és el seu cos de fraccions. Com que tot subanell de K és un anell íntegre, $\operatorname{Ker} f$ ha de ser un ideal primer de $\mathbb{Z}$. Si $\operatorname{Ker} f$ és trivial, $\operatorname{Im} f$ és isomorf a $\mathbb{Z}$, el cos primer de K és isomorf a $\mathbb{Q}$, i es diu que K té *característica zero*. Si $\operatorname{Ker} f = p\mathbb{Z}$, $\operatorname{Im} f$ és isomorf al cos finit $\mathbb{Z}/(p)$, el cos primer de K és $\operatorname{Im} f$, i es diu que K té *característica* p.

Si $\sigma\colon K \to L$ és una immersió, K i L tenen necessàriament la mateixa característica.

Immersió de Frobenius. Si K té característica $p > 0$, l'aplicació $\operatorname{Frob}_p\colon a \mapsto a^p$ és una immersió $K \to K$, que s'anomena *immersió de Frobenius*.

Un cos *perfecte* és un cos de característica zero o de característica $p > 0$ en que la immersió de Frobenius sigui un automorfisme.

Teorema 1.1. *Tot subgrup finit del grup multiplicatiu d'un cos és cíclic.*

PROVA: Sigui $G \subseteq K^*$ amb $|G| = n$. Sigui m el mínim comú múltiple dels ordres de tots els elements de G. Com que G és abelià ha de contenir un element d'ordre m; per tant, m divideix n. L'ordre de tot element $a \in G$ divideix m, $a^m = 1$, i a és una arrel a K del polinomi $X^m - 1 \in K[X]$. Com que un polinomi a un cos té, com a màxim, tantes arrels com el séu grau, $n \leqslant m$. Per tant, $n = m$ i G esta generat per un element d'ordre m. □

Aplicacions independents. Sigui S un conjunt i K un cos. El conjunt de les aplicacions $S \to K$, amb la suma i el producte per escalars naturals, és un K-espai vectorial. Una família d'aplicacions $S \to K$ és linealment independent quan ho és considerada a aquest espai vectorial.

Teorema 1.2. (*Teorema d'independència lineal de caracters*). *Sigui G un grup i $\{\chi_i\}_{i\in I}$ una colecció de caracters (homomorfismes de grups) $G \to K^*$ de G en el grup multiplicatiu d'un cos K. Si els χ_i són diferents, són independents (pensats com a aplicacions $G \to K$).*

PROVA: Suposem que no ho són. Sigui $\sum a_i\chi_i$, $a_i \in K$ gairebé tots nuls, una combinació lineal no trivial que, com a aplicació, sigui idènticament nul·la. Suposem que aquesta combinació té el nombre més petit possible de coeficients no nuls. Com que els χ_i prenen valors a K^*, almenys dos dels coeficients han de ser no nuls; siguin $a_j \neq 0$ i $a_k \neq 0$. Donats elements $g, h \in G$,

$$\sum a_i\chi_i(h)\chi_i(h^{-1}g) = \sum a_i\chi_i(g) = 0 \quad \forall g \in G.$$

Com que quan g recorre G també ho fa $h^{-1}g$, tenim una nova combinació lineal $\sum a_i\chi_i(h)\chi_i$ que dóna l'aplicació zero. Multiplicant la primera combinació per $\chi_j(h)$ i restant-li la segona obtenim la combinació

$$\sum b_i\chi_i = \sum a_i(\chi_j(h) - \chi_i(h))\chi_i,$$

que també és l'aplicació zero, i que té menys coeficients no nuls que la de partida ja que $a_i = 0 \Rightarrow b_i = 0$ i a més $b_j = a_j(\chi_j(h) - \chi_j(h)) = 0$. Per tant és la combinació trivial. Aleshores $b_k = a_k(\chi_j(h) - \chi_k(h)) = 0$ i $\chi_k(h) = \chi_j(h)$. Com que això val per tot $h \in G$, resulta que $\chi_k = \chi_j$ en contra de la hipòtesi que els caracters eren tots diferents. □

Corol·lari 1.3. (*Teorema d'independència lineal d'homomorfismes*). *Sigui $\{\sigma_i\}_{i\in I}$ una familia d'homomorfismes de cossos $K \to L$. Si són diferents, són L-independents.*

PROVA: S'aplica el teorema anterior als caracters $\sigma_i\colon K^* \to L^*$. □

2.– Extensions

Extensions. Sigui K un cos. Si K és un subcos del cos E, E s'anomena una *extensió* de K i es denota E/K. El cos E té una estructura natural de K-espai vectorial; la dimensió

corresponent és el *grau* de l'extensió, i es denota $[E : K]$. Una extensió és *finita* o *infinita* segons sigui el seu grau. Una sucessió de cossos on cadascun esta contingut al següent

$$K \subseteq F_1 \subseteq \cdots \subseteq F_r \subseteq E$$

és una *torre d'extensions*. Es denota també $E/F_r/\cdots/F_1/K$.

Un cos E tal que $L/E/K$ s'anomena *cos intermedi* de l'extensió L/K. Si E i F són cossos intermedis de L/K, la seva *composició* és el més petit subcos de L que els conté tots dos, i es denota EF. És clar que

$$EF = \{ \frac{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r}{\alpha'_1\beta'_1 + \cdots + \alpha'_s\beta'_s} \mid \alpha_i, \alpha'_i \in E,\ \beta_i, \beta'_i \in F,\ \text{denominador} \neq 0 \}.$$

L'extensió EF/F s'anomena l'*aixecament* de E/K sobre F.

La composició d'una família arbitraria de cossos intermedis es defineix de manera anàloga. Els cossos intermedis d'una extensió són un reticle amb la inclusió. La intersecció i la composició són, respectivament, l'ínfim i el suprem d'una família de subextensions.

Sigui $\sigma\colon K \to L$ un homomorfisme, i E/K, F/L extensions. Un homomorfisme $\tilde{\sigma}\colon E \to F$ és una *extensió* de σ si la seva restricció al cos K és σ. Si E i F són extensions de K, un K-homomorfisme $E \to F$ és un homomorfisme que deixi fixos els elements de K; o sigui, una extensió de la identitat $K \to K$. Els diagrames commutatius següents corresponen a aquestes situacions

$$\begin{array}{ccc} E & \xrightarrow{\tilde{\sigma}} & F \\ | & & | \\ K & \xrightarrow{\sigma} & L \end{array} \qquad\qquad \begin{array}{ccc} E & \longrightarrow & F \\ & \searrow \quad \swarrow & \\ & K & \end{array}$$

Lema 2.1. (*Construcció d'una extensió a partir d'una immersió*). *Sigui $\sigma\colon K \to E$ una immersió. Existeix una extensió E'/K i una extensió de σ a un isomorfisme $\tilde{\sigma}\colon E' \to E$.*

PROVA: Sigui S un conjunt (disjunt de K) amb el mateix cardinal que $E \setminus K^\sigma$, i $\phi\colon S \to E \setminus K^\sigma$ una bijecció qualsevol. Sigui $E' = S \cup K$ (com a conjunt) i $\tilde{\sigma}\colon E' \to E$ definida per

$$\tilde{\sigma}(x) = \begin{cases} \phi(x), & x \in S, \\ \sigma(x), & x \in K. \end{cases}$$

Aleshores $\tilde{\sigma}$ és una bijecció i es pot definir una suma i un producte a E' traslladant les operacions de E a través de $\tilde{\sigma}$. D'aquesta manera, E' té estructura de cos, és una extensió de K, i $\tilde{\sigma}$ és un isomorfisme de cossos que extén σ. □

Proposició 2.2. *El grau és multiplicatiu per torres d'extensions: si $E/F/K$,*

$$[E : K] = [E : F] \cdot [F : K].$$

En particular, si una extensió és finita, el grau de les extensions intermedies divideix el grau de l'extensió total.

PROVA: Sigui $\{\alpha_i\}_{i\in I}$ una K-base de F i $\{\beta_j\}_{j\in J}$ una F-base de E. Veguem que $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ és una K-base de E.

Si $x \in E$, siguin $x_j \in F$ quasi tots nuls tals que $x = \sum_{j\in J} x_j\beta_j$ i, per cada $j \in J$, siguin $a_{ij} \in K$ tals que $x_j = \sum_{i\in I} a_{ij}\alpha_i$. Si $x_j = 0$ tots els a_{ij} són zero i, en cas contrari, només un nombre finit són no nuls. En total hi ha només un nombre finit de a_{ij} no nuls, i $x = \sum a_{ij}(\alpha_i\beta_j)$. Per tant, el conjunt $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ genera E sobre K.

Sigui $\sum_{(i,j)\in I\times J} a_{ij}(\alpha_i\beta_j) = 0$, $a_{ij} \in K$ quasi tots nuls, una combinació lineal igual a zero. Aleshores $\sum_{j\in J}(\sum_{i\in I} a_{ij}\alpha_i)\beta_j = 0$; per independència lineal dels β_j sobre F tenim que $\sum_{i\in I} a_{ij}\alpha_i = 0 \ \ \forall j \in J$; per independència lineal dels α_i sobre K resulta que $a_{ij} = 0 \ \ \forall i \in I \ \ \forall j \in J$. □

Adjunció d'elements. Sigui E/K una extensió i $\alpha \in E$. Es denota $K[\alpha]$ el menor subanell de E que conté el cos K i l'element α, i $K(\alpha)$ el menor subcos. L'anell $K[\alpha]$ està format per totes les expresions polinòmiques en α a coeficients a K:

$$K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_r\alpha^r \mid a_i \in K, r \geqslant 0\} = \{f(\alpha) \mid f(X) \in K[X]\},$$

i el cos $K(\alpha)$ per totes les expresions racionals. Naturalment, $K(\alpha)$ és el cos de fraccions de $K[\alpha]$. El cos $K(\alpha)$ és el cos obtingut *adjuntant* α al cos K.

Anàlogament es defineixen l'anell $K[\alpha_1, \ldots, \alpha_r]$ i el cos $K(\alpha_1, \ldots, \alpha_r)$ per una família finita d'elements de E, i $K[S]$ i $K(S)$ per una família S arbitrària. El cos $K(S)$ és el cos obtingut *adjuntant* S al cos K. Els elements de $K[S]$ són les expresions polinòmiques en elements de S a coeficients a K

$$K[S] = \{\, f(\alpha_1, \ldots, \alpha_r) \mid \alpha_i \in S,\ f \in K[X_1, \ldots, X_r],\ r \geqslant 0\,\},$$

i els elements de $K(S)$ (que és el cos de fraccions de l'anell $K[S]$) són les expresions racionals $f(\alpha_1, \ldots, \alpha_r)/g(\beta_1, \ldots, \beta_s)$ amb denominador no nul.

Una extensió E/K és *finitament generada* si es pot obtenir adjuntant a K un conjunt finit d'elements i és *simple* si es pot obtenir adjuntant un sol element. En aquest darrer cas, si $E = K(\alpha)$, l'element α s'anomena *element primitiu* de l'extensió.

Tota extensió finita E/K és finitament generada, ja que s'obté adjuntant una K-base. Tota extensió finitament generada $K(\alpha_1, \ldots, \alpha_r)$ s'obté com una torre finita d'extensions simples

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \ldots K(\alpha_1, \ldots, \alpha_r).$$

Tota extensió és la composició de les seves subextensions finitament generades, i també és la composició de les seves subextensions simples.

Propietats heredades per adjunció. Moltes vegades ens interessen classes d'extensions E/K caracteritzades pel fet que tot element $\alpha \in E$ satisfa una certa propietat $\mathcal{P}$ (extensions

algebraiques, normals, separables, ...) i és important saber, quan $E = K(S)$, si es compleix la condició següent:

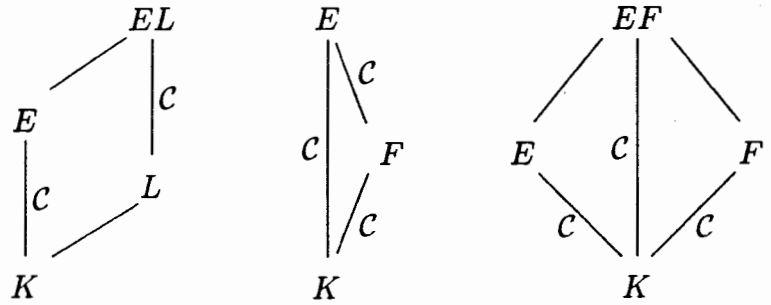
- Si tot element de S satisfa $\mathcal{P}$, aleshores tot element de E satisfa $\mathcal{P}$.

Quan es compleix aquesta condició es diu que la propietat $\mathcal{P}$ *s'hereda per adjunció.*

Classes distingides. Tractarem sovint amb classes d'extensions $\mathcal{C}$ (extensions finites, algebraiques, separables, de Galois, ...). Interessa saber si el fet de pertanyer a $\mathcal{C}$ es manté en certes situacions. Concretament, si $\mathcal{C}$ és una classe d'extensions, considerem les propietats:

- Si E/K és a $\mathcal{C}$ i EL/L és un aixecament sobre un cos L, aleshores EL/L és a $\mathcal{C}$.
- Siguin $E/F/K$. E/K és a $\mathcal{C}$ si i nomes si hi són E/F i F/K.
- Si E/K i F/K són a $\mathcal{C}$, també EF/K és a $\mathcal{C}$.

Els diagrames següents il·lustren les situacions



És clar que la tercera propietat és consequència de les dues primeres. Quan es compleixen totes tres es diu que la classe és *distingida.*

3.– Extensions algebraiques

Extensions algebraiques i trascendents. Sigui E/K una extensió. Un element $\alpha \in E$ és *algebraic* sobre K si és arrel d'algun polinomi no nul de $K[X]$, i *trascendent* en cas contrari. L'extensió E/K és *algebraica* si tot element de E és algebraic sobre K, i *trascendent* en cas contrari; o sigui, si E conté algun element trascendent sobre K. Si $E/F/K$ tot element de E algebraic sobre K ho és també sobre F, en particular si E/K és algebraica E/F també ho és.

Extensions simples. Considerem l'homomorfisme d'anells $\mathrm{av}_\alpha\colon K[X] \to E$ que a cada polinomi $f(X)$ li assigna l'element $f(\alpha)$. La imatge d'aquest homomorfisme és $K[\alpha]$, que és un anell íntegre, per tant el seu nucli és un ideal primer de $K[X]$. Hi ha dues possibilitats:

- Nucli trivial. Aleshores $K[\alpha]$ és isomorf a l'anell de polinomis $K[X]$, $K(\alpha)$ és isomorf al cos de funcions racionals $K(X)$, i l'extensió simple $K(\alpha)/K$ és de grau infinit. Correspon al cas que α és trascendent.
- Nucli no trivial. Sigui $f(X)$ un polinomi irreductible que el generi, $n = \deg f \geqslant 1$. Aleshores $K[\alpha]$ és isomorf al quocient $K[X]/(f(X))$, que és un cos, per tant $K(\alpha) = K[\alpha]$, l'extensió simple $K(\alpha)/K$ és finita de grau n, i les potències $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ són una K-base d'aquesta extensió. Correspon al cas que α és algebraic.

Si α és algebraic sobre K, el séu *polinomi irreductible* sobre K és el polinomi mònic de grau més petit de $K[X]$ que s'anul·la a α, i es denota $\mathrm{Irr}(\alpha, K; X)$. Aquest polinomi és el generador mònic del nucli de l'aplicació av_α i és, efectivament, un polinomi irreductible. S'anomena *grau* de l'element α sobre K al grau del polinomi $\mathrm{Irr}(\alpha, K; X)$. Si E/K és finita, el grau de α sobre K divideix $[E : K]$.

Proposició 3.1. *Siguin $K(\alpha)$ i $K(\beta)$ extensions simples d'un cos K. Existeix un K-isomorfisme $K(\alpha) \to K(\beta)$ que envia α a β si, i només si, α i β són tots dos trascendents sobre K o bé són tots dos algebraics i tenen el mateix polinomi irreductible.*

PROVA: Les condicions són òbviament necessàries ja que si σ és una K-immersió de cossos i α és arrel de $f(X) \in K[X]$ aleshores α^σ és arrel de $f^\sigma(X) = f(X)$. Per comprovar la suficiència, en el cas trascendent ambdues extensions són K-isomorfes a $K(X)$ i en el cas algebraic són K-isomorfes (via l'isomorfisme av) amb el cos $K[X]/(f(X))$ on $f(X)$ és el polinomi irreductible comú. □

Proposició 3.2. *Una extensió és finita si, i només si, és algebraica i finitament generada.*

PROVA: Sigui E/K finita de grau n. Si $\alpha \in E$, els $n+1$ elements $1, \alpha, \ldots, \alpha^n$ no poden ser K-independents. Una relació de K-dependència lineal entre aquests elements ens permet veure α com a arrel d'un polinomi no nul de $K[X]$. A més, E s'obté adjuntant a K una K-base.

Si l'extensió és simple $E = K(\alpha)$ amb α algebraic, és finita de grau el grau del polinomi $\mathrm{Irr}(\alpha, K; X)$. L'extensió algebraica $E = K(\alpha_1, \ldots, \alpha_r)$ s'obté com una torre finita d'extensions algebraiques simples adjuntant els elements α_i d'un en un i el resultat es dedueix a partir del cas simple i de la multiplicativitat del grau per torres. □

Proposició 3.3. *Si E/K és una extensió, els elements de E algebraics sobre K són un cos intermedi.*

PROVA: Siguin $\alpha, \beta \in E$ algebraics sobre K. Si α és arrel del polinomi no nul $f(X) \in K[X]$, $-\alpha$ ho és de $f(-X)$ i α^{-1} de $X^{\deg f} f(1/X)$. Considerem la torre d'extensions $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$. Cada graó és una extensió simple algebraica, per tant finita. Aleshores, l'extensió $K(\alpha, \beta)/K$ és finita ($\Rightarrow$ algebraica) i els elements $\alpha + \beta$ i $\alpha\beta$ pertanyen a aquest cos, per tant son algebraics sobre K. □

Proposició 3.4. *Sigui E/K algebraica. Tota K-immersió $E \to E$ és un isomorfisme.*

PROVA: Una immersió $\sigma : E \to E$ és, en particular, una aplicació K-lineal injectiva. Si E/K és finita, comptant dimensions es veu que σ és bijectiva.

Fem ara el cas general. Sigui $\alpha \in E$. Siguin $\alpha = \alpha_1, \ldots, \alpha_r$, $r \geqslant 1$, totes les arrels del polinomi $\mathrm{Irr}(\alpha, K; X)$ al cos E. Considerem l'extensió finita $F = K(\alpha_1, \ldots, \alpha_r)$. σ envia una arrel d'un polinomi de $K[X]$ a una arrel del mateix polinomi, per tant $F^\sigma \subseteq F$. Pel cas finit, $\sigma\colon F \to F$ és bijectiva. Per tant, $\alpha \in \mathrm{Im}\,\sigma$, i σ és exhaustiva. □

Proposició 3.5.

(a) *La propietat de ser algebraic s'hereda per adjunció.*

(b) *La classe de les extensions algebraiques és distingida.*

PROVA: (a) Sigui $E = K(S)$ amb els elements de S algebraics sobre K. Sigui F el subcos de E format per tots els elements algebraics sobre K. Aleshores $S \subseteq F$ i, per tant, $F = E$.

(b) Sigui E/K algebraica i EL/L un aixecament a un cos L. Cada element de E és algebraic sobre K i, per tant, ho és sobre L. Com que $EL = L(E)$, aplicant l'apartat anterior EL/L és algebraica.

Siguin $E/F/K$. Si E/K és algebraica ho són òbviament E/F i F/K. Recíprocament, suposem E/F i F/K algebraiques. Donat $\beta \in E$ siguin $\alpha_1, \ldots, \alpha_r \in F$ els coeficients del polinomi $\mathrm{Irr}(\beta, F; X)$. Aleshores $K(\alpha_1, \ldots, \alpha_r, \beta)$ és simple algebraica ($\Rightarrow$ finita) sobre $K(\alpha_1, \ldots, \alpha_r)$, que és finitament generada algebraica ($\Rightarrow$ finita) sobre K. Per tant $K(\alpha_1, \ldots, \alpha_r, \beta)/K$ és finita ($\Rightarrow$ algebraica) i β és algebraic sobre K. □

Teorema 3.6. (*Teorema de l'element primitiu*). *Una extensió finita és simple si, i només si, té un nombre finit de cossos intermedis.*

PROVA: Sigui E/K finita amb només un nombre finit de cossos intermedis. Si K és un cos finit E també ho és, E^* és ciclic i si α és un generador és clar que $E = K(\alpha)$. Suposem ara que K és infinit. Siguin $\alpha, \beta \in E$, considerem els (infinits) elements de la forma $\alpha + a\beta$ amb $a \in K$. Les extensions intermedies $K(\alpha + a\beta)$ no poden ser totes diferents en variar a. Suposem $K(\alpha + a\beta) = K(\alpha + b\beta)$ amb $a \neq b$. Aleshores aquesta extensió conté

$$\beta = \frac{(\alpha + a\beta) - (\alpha + b\beta)}{a - b} \qquad \text{i} \qquad \alpha = (\alpha + a\beta) - a\beta.$$

Per tant $K(\alpha, \beta) = K(\alpha + a\beta)$ és simple. Com que tota extensió finita és finitament generada per elements algebraics, si $E = K(\alpha_1, \ldots, \alpha_r)$ aplicant reiteredament la construcció anterior, veiem que E/K és simple. A més, sempre es pot trobar un element primitiu de la forma $\alpha_1 + a_2\alpha_2 + \cdots + a_r\alpha_r$.

Veguem ara el recíproc. Sigui $E = K(\alpha)$. Considerem l'aplicació que a cada cos intermedi F li fa correspondre el polinomi $f_F(X) = \mathrm{Irr}(\alpha, F; X)$. Com que $E = F(\alpha)$, $[E : F] = \deg f_F$. Tots aquests polinomis $f_F(X)$ divideixen $f_K(X)$ (sobre $E[X]$), per tant n'hi ha només un nombre finit. A més, F queda completament determinada pel polinomi f_F. En efecte, sigui F_0 l'extensió obtinguda en adjuntar a K els coeficients de

f_F. Clarament, $F_0 \subseteq F$ ja que F conté els coeficients en questió. El polinomi $f_F(X)$, que és irreductible $F[X]$, també ho és a $F_0[X]$. Per tant, $[E : F_0] = \deg f_F = [E : F]$, de on $F = F_0$. Aixi doncs, l'aplicació $F \mapsto f_F(X)$ és una aplicació injectiva del conjunt de cossos intermedis en un conjunt finit. □

4.– Cossos de descomposició

Teorema 4.1. *Si $f(X) \in K[X]$ és un polinomi no constant, existeix una extensió de K on f té una arrel.*

PROVA: Sigui $p(X)$ un factor irreductible de $f(X)$. El quocient de l'anell de polinomis $K[X]$ per l'ideal maximal generat per $p(X)$ és un cos $E = K[X]/(p(X))$, i tenim una immersió natural $\sigma : K \to K[X] \to E$. La classe de X és una arrel del polinomi $p^\sigma(X)$ a E. Pel lema 2.1 existeix una extensió E'/K i un isomorfisme $\tilde{\sigma}\colon E' \to E$ sobre σ. L'element $\tilde{\sigma}^{-1}(X)$ és una arrel de $p(X)$ a E'. □

Cos de descomposició. Sigui E/K una extensió. El polinomi $f(X) \in K[X]$ *descompon completament* a E si descompon a $E[X]$ com a producte de factors de grau 1; o sigui, si $f(X) = a_0(X - \alpha_1)\cdots(X - \alpha_n)$ on $a_0 \in K$ és el coeficient de grau més gran de f i $\alpha_1, \ldots, \alpha_n$ són elements de E (no necessariament diferents). Aplicant reiteradament el teorema anterior es veu que sempre existeix una extensió on un polinomi donat $f(X) \in K[X]$ descompon completament. A més, és clar que existeix una tal extensió que és finita de grau $\leqslant n!$, on $n = \deg f$.

L'extensió E/K és un *cos de descomposició* del polinomi $f(X) \in K[X]$ si f descompon completament a E i E és minimal amb aquesta propietat. Això equival a dir que $E = K(\alpha_1, \ldots, \alpha_n)$, on els α_i son les arrels de $f(X)$ a E. Tot polinomi té un cos de descomposició. Si E/K és una extensió en que el polinomi $f(X) \in K[X]$ descompon completament, existeix un únic cos intermedi que és un cos de descomposició de f: el cos $K(\alpha_1, \ldots, \alpha_r)$, on els $\alpha_i \in E$ son les arrels de $f(X)$. Si E és un cos de descomposició de $f(X) \in K[X]$ i F és un cos intermedi de l'extensió E/K, E tambe és un cos de descomposició del polinomi $f(X)$ vist com a polinomi amb coeficients a $F[X]$.

Sigui $T \subseteq K[X]$ un conjunt de polinomis. Un cos de descomposició de T és una extensió E/K on tots els polinomis de T descomponen completament, que sigui minimal amb aquesta propietat. Si tots els polinomis de T descomponen completament a E, existeix un únic cos intermedi de l'extensió E/K que sigui cos de descomposició de T: el cos obtingut adjuntant a K les arrels de tots els polinomis de T. Quan $T = \{f_1, \ldots, f_r\}$ és finit, un cos de descomposició de T és un cos de descomposició del polinomi producte $f = \prod_{i=1}^{r} f_i$; en particular, sempre existeix un tal cos.

Teorema 4.2. (*Existència de cossos de descomposició*). *Tot conjunt de polinomis té un cos de descomposició.*

PROVA: Sigui $T \subseteq K[X]$. Podem suposar que els polinomis de T són mònics. Considerem un conjunt de variables independents que contingui, per cada polinomi de T, tantes variables com el seu grau:

$$\boldsymbol{X} = \{ X_{f,i} \mid f \in T,\ 1 \leqslant i \leqslant \deg f \},$$

i sigui $R = K[\boldsymbol{X}]$ l'anell de polinomis corresponent. Per cada $f \in T$ i $1 \leqslant k \leqslant \deg f$, sigui $S_{f,k} \in R$ la k-èsima funció simètrica elemental en les variables $X_{f,i}$. A l'anell $R[X]$ es té, per cada $f \in T$, la identitat

$$X^n - S_{f,1}X^{n-1} + \cdots + (-1)^n S_{f,n} = (X - X_{f,1}) \cdots (X - X_{f,n}).$$

Siguin $a_{f,i} \in K$ els coeficients del polinomi f,

$$f(X) = X^n + a_{f,1}X^{n-1} + \cdots + a_{f,n-1}X + a_{f,n},$$

i sigui $\mathfrak{a} \subseteq R$ l'ideal generat per tots els elements $u_{f,k} = S_{f,k} - (-1)^k a_{f,k} \in R$. Si $\mathfrak{a} = R$ es tindria una identitat a R

$$g_1 u_{f_1,i_1} + \cdots + g_t u_{f_t,i_t} = 1, \quad g_j \in R.$$

Aleshores, si L/K és un cos de descomposició del conjunt finit de polinomis $\{f_1, \ldots, f_t\}$ podem considerar la identitat anterior a l'anell de polinomis $L[\boldsymbol{X}]$ i, substituint les variables $X_{f_j,i}$ corresponents als polinomis f_j per les arrels d'aquests polinomis a L, els u_{f_j,i_j} són zero, i resulta la identitat $0 = 1$ a $L[\boldsymbol{X}]$. Per tant, $\mathfrak{a}$ és un ideal propi de R.

Sigui $\mathfrak{m}$ un ideal maximal de R que contingui $\mathfrak{a}$. Aleshores $E = R/\mathfrak{m}$ és un cos, tenim una immersió natural $K \to R \to E$, i a E es tenen les identitats

$$f(X) = X^n + a_{f,1}X^{n-1} + \cdots + a_{f,n} = X^n - S_{f,1}X^{n-1} + \cdots + (-1)^n S_{f,n} =$$

$$(X - X_{f,1}) \cdots (X - X_{f,n}),$$

de manera que tot polinomi de T hi descompon completament. □

Cossos algebraicament tancats. Un cos Ω és *algebraicament tancat* si tot polinomi de $\Omega[X]$ descompon completament a Ω. És equivalent dir que tot polionomi de $\Omega[X]$ té alguna arrel a Ω, i també que tota extensió algebraica de Ω és trivial.

Una *clausura algebraica* d'un cos K és una extensió $\overline{K}/K$ algebraica que sigui algebraicament tancada.

Si Ω/K és una extensió algebraicament tancada i $T \subseteq K[X]$ existeix un únic cos intermedi de Ω/K que sigui un cos de descomposició de T, el cos obtingut adjuntant a K les arrels a Ω de tots els polinomis del conjunt T. En particular, Ω conté una única clausura algebraica de K.

Teorema 4.3. (*Existència de clausura algebraica*). *$\overline{K}/K$ és una clausura algebraica de K si, i només si, és un cos de descomposició del conjunt de polinomis $K[X]$. En particular, tot cos té una clausura algebraica.*

PROVA: Si $\overline{K}/K$ és una clausura algebraica tot polinomi de $K[X]$ descompon completament a $\overline{K}$ i tot element de $\overline{K}$ és arrel d'algun polinomi de $K[X]$. Per tant, $\overline{K} = K(\overline{K})$ és un cos de descomposició de $K[X]$.

Recíprocament, sigui $\overline{K}$ un cos de descomposició de $K[X]$. Donat $f(X) \in \overline{K}[X]$, sigui $E/\overline{K}$ un cos de descomposició. Aleshores E/K és algebraica i les arrels de f a E són arrels d'algun polinomi no nul a coeficients a K, per tant, pertanyen a $\overline{K}$ i $f(X)$ descompon completament a $\overline{K}$.

Com que tot conjunt de polinomis té un cos de descomposició, un cos sempre té una clausura algebraica. □

Teorema 4.4. (*Extensió d'immersions a un cos algebraicament tancat*). *Sigui $\sigma\colon K \to \Omega$ una immersió de K en un cos algebraicament tancat. Si E/K és una extensió algebraica, existeix una extensió de σ a una immersió $\tilde{\sigma}\colon E \to \Omega$.*

PROVA: Considerem en primer lloc el cas que $E = K(\alpha)$ és simple. Si $f(X) = \mathrm{Irr}(\alpha, K; X)$, el polinomi f^σ descompon completament a Ω; sigui β una arrel. Aleshores l'aplicació $g(\alpha) \mapsto g^\sigma(\beta)$ és una immersió $K(\alpha) \to \Omega$ (amb imatge $K^\sigma(\beta)$).

Per fer el cas general, considerem els parells (F, σ_F) formats per un cos intermedi F i una extensió $\sigma_F\colon F \to \Omega$ de σ, ordenats de manera que $(F_1, \sigma_{F_1}) \leqslant (F_2, \sigma_{F_2})$ si F_1 esta contingut a F_2 i σ_{F_2} extén σ_{F_1}. Si $\{(F_i, \sigma_{F_i})\}_{i\in I}$ és una cadena, el parell format pel cos $F = \bigcup_{i\in I} F_i$ i la immersió σ_F definida de manera que extengui les σ_{F_i} és una fita superior. Pel lema de Zorn, aquest conjunt té algun element maximal. Si (F, σ_F) és un element maximal, aleshores $F = E$ ja que si $\alpha \in E \setminus F$ gràcies al cas simple tindriem una extensió de σ_F al cos $F(\alpha)$ en contradicció amb la maximalitat de (F, σ_F). □

Corol·lari 4.5. (*Unicitat del cos de descomposició*). *Si E i F són cossos de descomposició d'un conjunt de polinomis $T \in K[X]$, existeix un K-isomorfisme $E \to F$. En particular, totes les clausures algebraiques d'un cos K són K-isomorfes.*

PROVA: Siguin $A = \{\alpha_i\}_{i\in I}$ i $B = \{\beta_i\}_{i\in I}$ les arrels dels polinomis del conjunt T a E i F, respectivament, de manera que $E = K(A)$ i $F = K(B)$. Sigui $\overline{F}/F$ una clausura algebraica, que també ho és de K. Pel teorema anterior existeix una K-immersió $\sigma\colon E \to \overline{F}$. Si α_i és arrel del polinomi f a E, aleshores α_i^σ és arrel del polinomi $f^\sigma = f$ a F i, per tant, pertany a B. Tenim $A^\sigma \subseteq B$ i, per tant, $E^\sigma \subseteq F$.

Hem demostrat que existeix una K-immersió $\sigma\colon E \to F$. Per simetria també existeix una K-immersió $\tau\colon F \to E$. Les composicions $\sigma\tau$ i $\tau\sigma$ són K-immersions $F \to F$ i $E \to E$, respectivament, i per la proposició 3.4 són isomorfismes. Per tant, σ i τ també ho són. □

5.– Extensions normals

Teorema 5.1. *Sigui N/K una extensió algebraica i $\overline{N}/N$ una extensió algebraicament tancada. Són equivalents:*
(a) *Per tot $\alpha \in N$, el polinomi $\mathrm{Irr}(\alpha, K; X)$ descompon completament a N.*
(b) *N és cos de descomposició d'un conjunt de polinomis $T \subseteq K[X]$.*
(c) *Per tota K-immersió $\sigma\colon N \to \overline{N}$, $N^\sigma = N$.*

PROVA: Suposem (a). Aleshores N és un cos de descomposició del conjunt de tots els polinomis $\mathrm{Irr}(\alpha, K; X)$ per $\alpha \in N$.

Suposem (b). Sigui $A \subseteq N$ el conjunt de les arrels dels polinomis de T. Aleshores $N = K(A)$. Com que tota K-immersió $\sigma\colon N \to \overline{N}$ envía un element de A a un element de A, $N^\sigma \subseteq N$ i, per la proposició 3.4, $N^\sigma = N$.

Suposem (c). Sigui $\alpha \in N$, i sigui β una arrel de $\mathrm{Irr}(\alpha, K; X)$ a $\overline{K}$. L'aplicació $g(\alpha) \mapsto g(\beta)$ és una K-immersió $K(\alpha) \mapsto \overline{K}$ amb imatge $K(\beta)$. Pel teorema 4.3 existeix una extensió d'aquesta immersió a una immersió $\sigma\colon N \to \overline{N}$. Aleshores $N^\sigma = N$ conté $\beta = \alpha^\sigma$ i, i totes les arrels de $\mathrm{Irr}(\alpha, K; X)$ estan contingudes a N.

Extensions normals. Una extensió algebraica N/K és *normal* si compleix les condicions equivalents del teorema anterior.

Si E/K és una extensió algebraica, una *clausura normal* és una extensió N/E tal que N/K sigui normal, minimal amb aquesta condició. Clarament, N/K és una clausura normal de E/K si, i només si, és un cos de descomposició sobre E del conjunt de polinomis $\mathrm{Irr}(\alpha, K; X)$ per tot $\alpha \in E$. En particular, tota extensió algebraica E/K té una clausura normal, que és única llevat de K-isomorfisme. Si M/E és una extensió tal que M/K és normal, existex una única subextensió N/E que sigui una clausura normal de E/K.

Si E/K és finita, $E = K(\alpha_1, \ldots, \alpha_r)$, i f és el producte dels polinomis $\mathrm{Irr}(\alpha_i, K; X)$, una clausura normal de E/K és un cos de descomposició de f. En particular, una clausura normal d'una extensió finita és una extensió finita.

Si E/K és algebraica i Ω/E és un cos algebraicament tancat, la composició de tots els cossos $E^\sigma \subseteq \Omega$ per totes les K-immersions $\sigma\colon E \to \Omega$ és una clausura normal de E/K.

Proposició 5.2.
(a) *Si $E = K(S)$ i per cada $\alpha \in S$ el polinomi $\mathrm{Irr}(\alpha, K; X)$ descompon completament a E, E/K és normal.*
(b) *La classe de les extensions normals és tancada per aixecament.*
(d) *Siguin $E/F/K$. Si E/K és normal E/F també ho és.*
(c) *La classe de les extensions normals és tancada per composició.*

PROVA: (a) En efecte, E és un cos de descomposició d'aquests polinomis.

(b) Sigui N/K una extensió normal i NL/L un aixecament. Per cada $\alpha \in N$, el polinomi $\mathrm{Irr}(\alpha, K; X)$ descompon completament a N i, per tant, a NL. Com que $NL = L(N)$, aplicant l'apartat anterior resulta que NL/L és normal.

(c) Evident.

(d) Si N/K i M/K extensions normals, $MN = K(M \cup N)$ i apliquem l'apartat (a). □

Exemple. Sigui α una arrel real del polinomi $X^4 - 2 \in \mathbb{Q}[X]$. Les quatre arrels complexes d'aquest polinomi són $\alpha, -\alpha, i\alpha, -i\alpha$. Considerem la torre d'extensions

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^2) \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, i) \subset \mathbb{C}.$$

L'extensió $\mathbb{Q}(\alpha, i)/\mathbb{Q}$ és normal, ja que és un cos de descomposició del polinomi $X^4 - 2$, en canvi $\mathbb{Q}(\alpha)/\mathbb{Q}$ no ho és. Les extensions $\mathbb{Q}(\alpha^2)/\mathbb{Q}$ i $\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha^2)$ són normals ja que són, respectivament, cossos de descomposció dels polinomis $X^2 - 2 \in \mathbb{Q}[X]$ i $X^2 - \alpha^2 \in \mathbb{Q}(\alpha^2)[X]$. Amb aquest exemple es veu que podem tenir una torre $E/F/K$ amb E/K normal tal que F/K no ho sigui, i amb E/F i F/K normals però tal que E/K no ho sigui. □

6.– Separabilitat.

Polinomis i extensions separables. Un polinomi irreductible $f(X) \in K[X]$ és *separable* si totes les seves arrels a un cos de descomposició són simples; és a dir, tenen multiplicitat 1. Equival a dir que és relativament primer amb la seva derivada $f'(X)$. El polinomi és *inseparable* en cas contrari. La definició no depèn del cos de descomposició escollit, ja que tots els cossos de descomposició són K-isomorfs. Un polinomi qualsevol és separable quan ho són tots els seus factors irreductibles.

Sigui E/K una extensió algebraica. Un element $\alpha \in E$ és *separable* sobre K si ho és el seu polinomi irreductible. Si $E/F/K$ és una torre d'extensions algebraiques, un element $\alpha \in E$ separable sobre K també és separable sobre F ja que $\mathrm{Irr}(\alpha, F; X)$ divideix $\mathrm{Irr}(\alpha, K; X)$.

L'extensió E/K és separable si tot element de E és separable sobre K.

Proposició 6.1. *Si* $\operatorname{car} K = 0$ *tot polinomi és separable. Si* $\operatorname{car} K = p > 0$ *un polinomi irreductible* $f(X) \in K[X]$ *és inseparable si, i només si, és de la forma* $f(X) = g(X^p)$ *per algun polinomi* g.

PROVA: Sigui $d(X) = (f(X), f'(X))$ el màxim comú divisor. Com que $f(X)$ és irreductible, $d(X)$ només pot ser 1 o $f(X)$, llevat d'unitats. Com que $\deg f' < \deg f$,

$$d(X) = 1 \Leftrightarrow f'(X) \neq 0, \quad d(X) = f(X) \Leftrightarrow f'(X) = 0.$$

Si $f(X) = a_0 + a_1X + \cdots + a_nX^n$, $n \geqslant 1$, $f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$.

Si $\operatorname{car} K = 0$, f' no pot ser zero ja que $na_n \neq 0$, i en caracteristica és zero tot polinomi és separable.

Si $\operatorname{car} K = p$, $f' = 0$ si, i només si, els únics coeficients no nuls a_i del polinomi corresponen a potències de X d'exponent múltiple de p; això equival a dir que existeix un polinomi $g(X) \in K[X]$ tal que $f(X) = g(X^p)$. □

Lema 6.2. *Sigui* $\operatorname{car} K = p > 0$. *Si* $f(X) \in K[X]$ *és un polinomi irreductible, totes les seves arrels a un cos de descomposició tenen la mateixa multiplicitat, que és una potència de* p.

PROVA: Sigui E/K un cos de descomposició de $f(X)$. Sigui $t \geqslant 0$ l'enter mes gran tal que existeix un polinomi $g(X) \in K[X]$ amb $f(X) = g(X^{p^t})$; o sigui, $g(X)$ no és igual a $h(X^p)$ per cap polinomi $h(X) \in K[X]$. Aleshores $g(X)$ és irreductible ja que una factorització no trivial de g proporcionaria una factorització no trivial de f i, per la proposició anterior és separable.

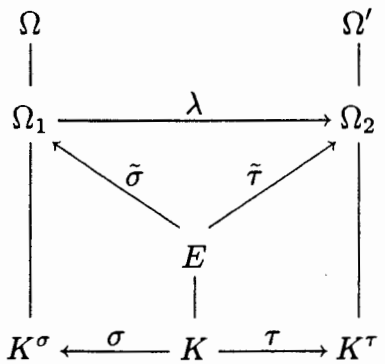
El polinomi g descompon completament a E ja que les seves arrels són potències p^t-èssimes de les arrels de f. Siguin $g(X) = (X - \alpha_1)\cdots(X - \alpha_s)$ la seva factorització a $E[X]$, amb les α_i totes diferents ja que és separable. Aleshores $f(X) = g(X^{p^t}) = (X^{p^t} - \alpha_1)\ldots(X^{p^t} - \alpha_s)$. Les arrels de f ho són d'algun dels polinomis de la dreta. Sigui β_i arrel de $X^{p^t} - \alpha_i$. Els β_i són tots diferents ja que els α_i ho són, i tenim la factorització

$$f(X) = g(X^{p^t}) = (X - \beta_1)^{p^t} \cdots (X - \beta_s)^{p^t}.$$

Per tant, les arrels de f a E tenen totes la mateixa multiplicitat p^t. □

Lema 6.3. *Sigui* E/K *una extensió algebraica,* $\sigma\colon K \to \Omega$ *una immersió en un cos algebraicament tancat. El nombre d'immersions* $\tilde{\sigma}\colon E \to \Omega$ *sobre* σ *només depèn de l'extensió* E/K; *o sigui, és independent del cos* Ω *i de la immersió* σ.

PROVA: Sigui $\tau\colon K \to \Omega'$ una altra immersió en un cos algebraicament tancat. Siguin Ω_1 i Ω_2 les clausures algebraiques de K^σ i de K^τ dins de Ω i Ω' respectivament. Sigui $\lambda\colon \Omega_1 \to \Omega_2$ un isomorfisme sobre $\tau\sigma^{-1}$. Les immersions $\tilde{\sigma}$ sobre σ i $\tilde{\tau}$ sobre τ tenen les imatges dins de Ω_1 i Ω_2, respectivament, i tenim un diagrama commutatiu



Aleshores l'aplicació $\tilde{\sigma} \mapsto \lambda\tilde{\sigma}$ és una bijecció entre les extensions de σ i les extensions de τ, amb inversa $\tilde{\tau} \mapsto \lambda^{-1}\tilde{\tau}$. □

Grau de separabilitat. Sigui $f(X) \in K[X]$ un polinomi irreductible. El *grau de separabilitat* de f és el nombre d'arrels diferents que té a un cos de descomposició, i el *grau d'inseparabilitat* la multiplicitat d'aquestes arrels (la mateixa per totes, segons el lema 6.2). El grau d'inseparabilitat és 1 per característica zero i és una potència de p per característica $p > 0$. El producte d'ambdos graus és el grau del polinomi.

Sigui E/K una extensió algebraica i Ω/E una clausura algebraica. El *grau de separabilitat* de E/K és el nombre de K-immersions de $E \to \Omega$. Pel lema 6.3 el grau de separabilitat només depèn de l'extensió E/K i no de la clausura algebraica Ω escollida. Es denota $[E : K]_s$.

Clarament, el grau de separabilitat de l'extensió simple $K(\alpha)/K$ és el grau de separabilitat del polinomi $\mathrm{Irr}(\alpha, K; X)$, ja que les K-immersions $K(\alpha) \to \Omega$ es corresponen amb les diferents arrels de $\mathrm{Irr}(\alpha, K; X)$ a Ω.

Teorema 6.4. *El grau de separabilitat és multiplicatiu per torres d'extensions: si $E/F/K$ és una torre d'extensions algebraiques,*

$$[E : K]_s = [E : F]_s \cdot [F : K]_s.$$

PROVA: Sigui Ω/E una clausura algebraica. Naturalment, Ω és també clausura algebraica de F i de K. Hi ha $[F : K]_s$ K-immersions $\sigma\colon F \to \Omega$. Per cada σ, el nombre d'immersions $\tilde{\sigma}\colon E \to \Omega$ sobre σ és independent de σ (lema 6.3) i, per tant, és igual al grau de separabilitat $[E : F]_s$, que per definició és el nombre d'extensions de $\sigma = Id$.

Tota K-immersió $E \to \Omega$ és extensió a E d'una K-immersió $\sigma\colon F \to \Omega$. □

Corol·lari 6.5. *Si E/K és una extensió finita, el grau de separabilitat divideix el grau, i el quocient $[E : K]_i = [E : K]/[E : K]_s$, que s'anomena grau d'inseparabilitat, és una potència de la característica.*

PROVA: En el cas que $E = K(\alpha)$ sigui simple és immediat. El cas general es redueix al simple tenint en compte que una extensió finita s'obté com una torre finita d'extensions simples, i utilitzant les multiplicativitats del grau i del grau de separabilitat. □

Proposició 6.6. *Una extensió finita és separable si, i només si, el grau de separabilitat és igual al grau. O sigui; si, i només si, el grau d'inseparabilitat és* 1.

PROVA: Si l'extensió és simple és immediat. El cas general es redueix al simple fent servir les multiplicativitats del grau i grau de separabilitat. □

Proposició 6.7. *La separabilitat s'hereda per adjunció. La classe de les extensions separables és distingida.*

PROVA: Sigui $E = K(S)$ amb tot $\alpha \in S$ separable sobre K. Si S és un conjunt finit, E s'obté com una torre finita d'extensions simples separables i, per tant, és separable. Pel cas general, tot element $\alpha \in E$ pertany a $K(S_0)$ per algun subconjunt finit $S_0 \subseteq S$, $K(S_0)/K$ és separable i per tant α és separable sobre K

Sigui E/K separable i EL/L és un aixecament sobre L. Cada $\alpha \in E$ és separable sobre K i, per tant, sobre L. Com que $EL = L(E)$ i la separabilitat s'hereda per adjunció, EL/L és separable.

Sigui $E/F/K$. Si E/K és separable, clarament ho és F/K i, com que per $\alpha \in E$ el polinomi $\mathrm{Irr}(\alpha, F; X)$ divideix $\mathrm{Irr}(\alpha, K; X)$ també E/F és separable. Recíprocament, suposem que E/F i F/K són separables. Si E/K és finita, per multiplicativitat dels graus és separable. El cas general es redueix al cas finit tenint en compte que tot element $\beta \in E$ pertany a l'extensió finita $K(\alpha_1, \ldots, \alpha_n, \beta)$ on els $\alpha_i \in F$ són els coeficients del polinomi $\mathrm{Irr}(\alpha, F; X)$. □

7.– Extensions de Galois

Grups d'automorfismes. Sigui E/K una extensió. Els K-automorfismes de E formen un grup, que s'anomena *grup de Galois* de l'extensió, i es denota $\mathrm{Gal}(E/K)$. Quan E/K és normal, els elements de $\mathrm{Gal}(E/K)$ són les K-immersions $E \to \overline{E}$ de E en una clausura algebraica.

Si G és un grup d'automorfismes d'un cos E, G opera sobre E i el conjunt de punts fixos d'aquesta acció $\{\alpha \in E \mid \alpha^\sigma = \alpha \ \ \forall \sigma \in G\}$ és un subcos de E, que s'anomena *cos fix* de G, i es denota E^G.

Sigui E/K una extensió i $G = \mathrm{Gal}(E/K)$ el seu grup de Galois. Sigui $\mathcal{F} = \mathcal{F}(E/K)$ el reticle dels cossos intermedis de l'extensió i $\mathcal{H} = \mathcal{H}(G)$ el reticle de subgrups del grup G. Tenim aplicacions

$$\begin{array}{ccc} \mathcal{F} & \to & \mathcal{H} \\ F & \mapsto & \mathrm{Gal}(E/F) \end{array} \qquad \begin{array}{ccc} \mathcal{H} & \to & \mathcal{F} \\ H & \mapsto & E^H \end{array}$$

que canvien l'ordre de les inclusions,

$$F_1 \subseteq F_2 \Rightarrow \mathrm{Gal}(E/F_2) \subseteq \mathrm{Gal}(E/F_1), \qquad H_1 \subseteq H_2 \Rightarrow E^{H_2} \subseteq E^{H_1},$$

i tals que

$$F \subseteq E^{\mathrm{Gal}(E/F)}, \qquad H \subseteq \mathrm{Gal}(E/E^H).$$

Extensions de Galois. Una extensió algebraica és *de Galois* si és normal i separable. Una extensió *abeliana* (resp. *cíclica*) és una extensió de Galois amb grup de Galois abelià (resp. cíclic).

Proposició 7.1. *Si l'extensió E/K és de Galois, aleshores $E^{\mathrm{Gal}(E/K)} = K$.*

PROVA: La inclusió $K \subseteq E^{\mathrm{Gal}(E/K)}$ es compleix sempre. Sigui $\alpha \in E^{\mathrm{Gal}(E/K)}$. Tota K-immersió $\sigma\colon K(\alpha) \to \overline{E}$ s'extén a una K-immersió $\tilde{\sigma}\colon E \to \overline{E}$. Com que E/K és normal, $\tilde{\sigma} \in \mathrm{Gal}(E/K)$, $\tilde{\sigma}$ deixa fix α i σ és la identitat. Per tant, $[K(\alpha) : K]_s = 1$. Com que l'extensió és separable, $[K(\alpha) : K] = 1$ i $\alpha \in K$. □

Proposició 7.2. *Una extensió finita E/K és de Galois si, i només si,*

$$|\,\mathrm{Gal}(E/K)\,| = [E : K].$$

PROVA: Si E/K és una extensió finita, es tenen desigualtats

$$|\,\mathrm{Gal}(E/K)\,| \leqslant [E : K]_s \leqslant [E : K].$$

La primera és una igualtat si, i només si, E/K és normal i la segona ho és si, i només si, E/K és separable. □

Teorema 7.3. (*Teorema d'Artin*). *Si G és un grup finit d'automorfismes d'un cos E i $K = E^G$ és el seu cos fix, l'extensió E/K és de Galois amb grup de Galois G.*

PROVA: Sigui $\alpha \in E$. Siguin $\alpha_1, \ldots, \alpha_r$ les diferents imatges de l'element α pels automorfismes de G (o sigui, l'òrbita de α per l'acció de G). Considerem el polinomi $f(X) = (X - \alpha_1)\cdots(X - \alpha_r) \in E[X]$. Per tot $\sigma \in G$, els elements $\alpha_1^\sigma, \ldots, \alpha_r^\sigma$ són una permutació de $\alpha_1, \ldots, \alpha_r$, per tant $f^\sigma(X) = f(X)$. Com que els coeficients de f queden fixos per tot element de G, $f(X) \in K[X]$. Aleshores α és una arrel d'un polinomi separable de $K[X]$ que descompon completament a E; per tant, E/K és algebraica, normal i separable.

El grup G és un subgrup de $\mathrm{Gal}(E/K)$, que per la proposició anterior té cardinal $[E : K]$. Per veure que són iguals només cal comprovar que $|G| = [E : K]$. Siguin $\sigma_1, \ldots, \sigma_n$ els elements de G. Sigui $m > n$ i $\alpha_1, \ldots, \alpha_m$ elements de E. Considerem el sistema lineal homogeni de n equacions i m incògnites:

$$\begin{array}{ccccccc} \alpha_1^{\sigma_1} X_1 & + & \ldots & + & \alpha_m^{\sigma_1} X_m & = & 0 \\ \ldots & & \ldots & & \ldots & & \\ \alpha_1^{\sigma_n} X_1 & + & \ldots & + & \alpha_m^{\sigma_n} X_m & = & 0 \end{array}$$

Les solucions d'aquest sistema són un subespai vectorial no trivial de E^m. Aplicar un automorfisme $\sigma \in G$ al sistema en permuta les equacions i el transforma en si mateix, per tant si $x = (x_1, \ldots, x_m)$ és una solució, $x^\sigma = (x_1^\sigma, \ldots, x_m^\sigma)$ també ho és. Sigui x una solució

no trivial amb el nombre de coordenades no nul·les més petit possible; si $x_k \neq 0$, dividint per x_k podem suposar que $x_k = 1$. Aleshores $y = x - x^\sigma$ també és solució del sistema, i té menys coordenades no nul·les que x ja que $x_i = 0 \Rightarrow y_i = 0$ i, a més, $y_k = 1 - 1^\sigma = 0$. Per tant y és la solució trivial i $x^\sigma = x$. Com que les coordenades x queden fixes per tot element de G, són elements de K. Aleshores l'equació del sistema que correspon a la identitat de G proporciona una relació de dependència lineal sobre K entre els elements $\alpha_1, \ldots, \alpha_m$. Per tant, $[E : K] \leqslant |G|$. □

Teorema 7.4. (*Teorema fonamental de la Teoria de Galois*). *Sigui E/K una extensió de Galois, $\mathcal{F}$ el reticle de cossos intermedis, i $\mathcal{H}$ el reticle de subgrups de* $\mathrm{Gal}(E/K)$. *L'aplicació $\mathcal{F} \to \mathcal{H}$ que assigna a cada cos intermedi el séu grup de Galois és injectiva i, si l'extensió és finita, és exhaustiva.*

PROVA: Si F_1 i F_2 són cossos intermedis, les extensions E/F_1 i E/F_2 són de Galois i, aplicant la proposició 1.1,

$$\mathrm{Gal}(E/F_1) = \mathrm{Gal}(E/F_2) \quad \Rightarrow \quad F_1 = E^{\mathrm{Gal}(E/F_1)} = E^{\mathrm{Gal}(E/F_2)} = F_2.$$

Si l'extensió és finita, $\mathrm{Gal}(E/K)$ és finit. Tot subgrup $H \subseteq \mathrm{Gal}(E/K)$ és finit i, pel teorema d'Artin, $H = \mathrm{Gal}(E/E^H)$. □

Corol·lari 7.5. *Tota extensió finita separable té un element primitiu.*

PROVA: Si E/K és finita separable, sigui N/K una clausura normal. Aleshores N/K és de Galois finita i, pel teorema anterior, té només un nombre finit de cossos intermedis (tants com subgrups del grup finit $\mathrm{Gal}(N/K)$). Aleshores E/K té només un nombre finit de cossos intermedis i, pel teorema de l'element primitiu, té un element primitiu. □

Conjugats. Sigui E/K una extensió i $G = \mathrm{Gal}(E/K)$. El grup G opera per l'esquerra sobre els cossos intermedis

$$(\sigma, F) \mapsto F^\sigma,$$

i sobre els subgrups de G per conjugació

$$(\sigma, H) \mapsto \sigma H \sigma^{-1}.$$

Les aplicacions $F \mapsto \mathrm{Gal}(E/F)$ i $H \mapsto E^H$ són compatibles amb aquestes accions; o sigui,

$$\mathrm{Gal}(E/F^\sigma) = \sigma \,\mathrm{Gal}(E/F)\sigma^{-1}, \qquad E^{\sigma H \sigma^{-1}} = (E^H)^\sigma.$$

És per aquest motiu que dos cossos intermedis d'una extensió E/K s'anomenen *conjugats* si existeix un K-automorfisme que envia l'un a l'altre. El mateix per elements: dos elements de E són *conjugats* (sobre K) si existeix un K-automorfisme que envii l'un a l'altre; en el cas algebraic és el mateix que dir que tenen el mateix polinomi irreductible sobre K.

Teorema 7.6. *Si E/K és una extensió de Galois i F un cos intermedi, l'extensió F/K és de Galois si, i només si,* $\mathrm{Gal}(E/F)$ *és un subgrup normal de* $\mathrm{Gal}(E/K)$. *En tal cas, la restricció* $\mathrm{Gal}(E/K) \to \mathrm{Gal}(F/K)$ *és un epimorfisme de grups amb nucli* $\mathrm{Gal}(E/F)$.

PROVA: L'extensió F/K sempre és separable, de manera que és de Galois si, i només si, és normal. Totes les K-immersions $F \mapsto \overline{E}$ s'obtenen per restricció d'elements de $\mathrm{Gal}(E/K)$, per tant F/K és normal si, i només si, $F^\sigma = F$ per tot $\sigma \in \mathrm{Gal}(E/K)$. Tenint en compte la injectivitat de $F \mapsto \mathrm{Gal}(E/F)$, aquesta condició és equivalent a que $\sigma\,\mathrm{Gal}(E/F)\sigma^{-1} = \mathrm{Gal}(E/F)$ per tot $\sigma \in \mathrm{Gal}(E/K)$. □

Teorema 7.7.

(a) *Tot aixecament EL/L d'una extensió de Galois E/K és de Galois, i la restricció* $\mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/K)$ *és un monomorfisme.*

(b) *La composició d'extensions de Galois E/K i F/K és de Galois, i la restricció a les components* $\mathrm{Gal}(EF/K) \mapsto \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ *és un monomorfisme.*

PROVA: (a) Com que la normalitat i la separabilitat es mantenen per aixecament, la condició de ser de Galois també. Que la restricció és un monomorfisme és evident.

(b) Com que la normalitat i la separabilitat es mantenen per composició, la condició de ser de Galois també. Que l'aplicació és un monomorfisme és evident. □

Grup de Galois d'un polinomi. El grup de Galois d'un polinomi $f(X) \in K[X]$ és el grup dels K-automorfismes d'un cos de descomposició E/K, $\mathrm{Gal}(E/K)$. Com que tots els cossos de descomposició són K-isomorfs, aquest grup de Galois queda determinat llevat d'isomorfisme.

Siguin $\alpha_1, \ldots, \alpha_n$ les diferents arrels de $f(X)$ a E. Aleshores $E = K(\alpha_1, \ldots, \alpha_n)$ i cada $\sigma \in \mathrm{Gal}(E/K)$ permuta les arrels α_i. Cada $\sigma \in \mathrm{Gal}(E/K)$ proporciona un element de $\mathfrak{S}_n$, anomenem-lo també σ, determinat per la condició $\alpha_i^\sigma = \alpha_{\sigma(i)}$. D'aquesta manera tenim una aplicació

$$\mathrm{Gal}(E/K) \to \mathfrak{S}_n$$

que és injectiva, ja que una K-immersió $E \to E$ queda completament determinada per l'efecte que té sobre les α_i.

La imatge d'aquesta aplicació consisteix en les permutacions $\sigma \in \mathfrak{S}_n$ tals que per tot polinomi $g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$,

$$g(\alpha_1, \ldots, \alpha_n) = 0 \quad \Rightarrow \quad g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$$

o, el que és equivalent, tals que per tot polinomi $g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$,

$$g(\alpha_1, \ldots, \alpha_n) = a \in K \quad \Rightarrow \quad g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = a.$$

8.– Extensions cícliques

Arrels de la unitat. Sigui K un cos i $n \geqslant 1$. Les *arrels n-èsimes de la unitat* sobre K son les arrels del polinomi $X^n - 1$ a un cos de descomposició. Denotem per μ_n el conjunt d'aquestes arrels. Aquest conjunt és òbviament un grup, subgrup finit del grup multiplicatiu del cos de descomposició, per tant cíclic. Els seus generadors s'anomenen *arrels n-èsimes primitives de la unitat*. Si K té característica zero, μ_n conté n elements, si té característica p i $n = p^r n_0$ amb p no dividint n_0 aleshores μ_n conté n_0 elements i, de fet, $\mu_n = \mu_{n_0}$.

Si $\overline{K}$ és una clausura algebraica de K, podem considerar totes les arrels de la unitat a $\overline{K}$; o sigui, les arrels dels polinomis $X^n - 1$ per tot enter n. Si denotem per $\mu \subset \overline{K}^*$ el conjunt de totes aquestes arrels, μ és un grup abelià que conté el grup μ_n per tot n. Tot element de μ és una arrel primitiva n-èsima de la unitat per un únic $n \geqslant 1$.

Extensions ciclotòmiques. Sigui n primer amb la característica de K i ζ_n una arrel primitiva n-èsima de la unitat sobre K. L'extensió $K(\zeta_n) = K(\mu_n)$ (que pot ser trivial) s'anomena *n-èsima extensió ciclotòmica* de K, i és clarament una extensió normal i separable de K. Per cada $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$, ζ_n^σ és una altra arrel primitiva n-èsima de la unitat, per tant existeix un enter $\theta(\sigma)$, determinat només mòdul n, tal que $\zeta_n^\sigma = \zeta_n^{\theta(\sigma)}$. Com que ζ_n^σ és primitiva, necessàriament $(n, \theta(\sigma)) = 1$. A més, $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$. Per tant tenim un homomorfisme injectiu:

$$\theta\colon \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^*.$$

de manera que el grup $\mathrm{Gal}(K(\zeta_n)/K)$ és isomorf a un subgrup del grup multiplicatiu mòdul n. En particular, és abelià d'ordre dividint $\varphi(n)$.

Norma i traça. Sigui E/K una extensió finita de Galois amb grup de Galois G. Si $\alpha \in E$, la *norma* i la *traça* de α es defineixen com

$$N_{E/K}(\alpha) = \prod_{\sigma \in G} \alpha^\sigma, \qquad \mathrm{Tr}_{E/K}(\alpha) = \sum_{\sigma \in G} \alpha^\sigma.$$

La norma és un homomorfisme de grups $E^* \to K^*$ i la traça és una aplicació K-lineal $E \to K$. Per definició, la traça és una combinació lineal no trivial d'homomorfismes diferents $E \to E$; pel Teorema d'independència lineal d'homomorfismes, no pot ser idènticament nul·la.

Teorema 8.1. *(Teorema 90 de Hilbert). Sigui E/K una extensió cíclica de grau n, $G = \mathrm{Gal}(E/K)$, i $\sigma \in G$ un generador. Un element $\beta \in E^*$ té norma $N_{E/K}(\beta) = 1$ si, i només si, existeix un element $\alpha \in E^*$ tal que $\beta = \alpha/\alpha^\sigma$.*

PROVA: Si $\beta = \alpha/\alpha^\sigma$ és clar que $N(\beta) = 1$. Suposem que $N(\beta) = 1$. Els elements de G són $\mathrm{Id}, \sigma, \ldots, \sigma^{n-1}$ i, pel teorema d'independència lineal d'homomorfismes, són E-independents com a aplicacions $E \to E$. Per tant, la combinació lineal a coeficients no

nuls

$$f = \mathrm{Id} + \beta\sigma + \beta^{\mathrm{Id}+\sigma}\sigma^2 + \cdots + \beta^{\mathrm{Id}+\sigma+\cdots+\sigma^{n-2}}\sigma^{n-1}$$

és una aplicació no trivial $E \to E$ (la notació $\beta^{\tau_1+\tau_2}$ vol dir $\beta^{\tau_1}\beta^{\tau_2}$, i es compleixen les regles habituals de l'exponenciació). Sigui $\gamma \in E$ un element amb $f(\gamma) \neq 0$; diguem $\alpha = f(\gamma)$. De la identitat

$$\alpha = \gamma + \beta\gamma^{\sigma} + \beta^{\mathrm{Id}+\sigma}\gamma^{\sigma^2} + \cdots + \beta^{\mathrm{Id}+\sigma+\cdots+\sigma^{n-2}}\gamma^{\sigma^{n-1}},$$

tenint en compte que $\beta^{\mathrm{Id}+\sigma+\cdots+\sigma^{n-1}} = N(\beta) = 1$, se'n dedueix que $\alpha^{\sigma}\beta = \alpha$. □

Teorema 8.2. (*Extensions cícliques de grau primer amb la característica*). *Sigui K un cos i n un enter primer amb la seva característica. Suposem que $\mu_n \in K$. Aleshores:*

(a) *Si E/K és una extensió cíclica de grau n, $E = K(\alpha)$, amb α arrel d'algun polinomi $X^n - a \in K[X]$.*

(b) *Sigui $a \in K$ i α una arrel de $X^n - a$ a un cos de descomposició. L'extensió $K(\alpha)/K$ és cíclica de grau d, el més petit divisor de n tal que $\alpha^d \in K$.*

PROVA: (a) Sigui $\zeta_n \in K$ una arrel primitiva n-èsima de la unitat i σ un generador de $G = \mathrm{Gal}(E/K)$. Pel teorema 90 de Hilbert (aplicat a ζ_n^{-1}) existeix un element $\alpha \in E$ tal que $\zeta_n = \alpha^{\sigma}/\alpha$. Aleshores, els elements $\alpha^{\sigma^i} = \zeta_n^i\alpha$ són diferents per $i = 1, \ldots, n$; com que aquests elements són els conjugats de α, α té grau n sobre K, i $E = K(\alpha)$. A més, $(\alpha^n)^{\sigma} = (\alpha^{\sigma})^n = (\zeta_n\alpha)^n = \alpha^n$, de manera que α^n és fix per G i pertany a K; diguem $a = \alpha^n \in K$, aleshores α és arrel de $X^n - a$.

(b) Els elements $\zeta_n^i\alpha \in K(\alpha)$, per $i = 0, \ldots, n-1$, són les diferents arrels de $X^n - a$ a $K(\alpha)$, per tant, $K(\alpha)$ és un cos de descomposició d'aquest polinomi, clarament separable sobre K. Sigui $G = \mathrm{Gal}(K(\alpha)/K)$. Els elements de G queden completament determinats per la imatge de α. Per cada $\sigma \in G$ existeix un enter $i = i(\sigma)$, determinat només mòdul n, tal que $\alpha^{\sigma} = \zeta_n^i\alpha$. Clarament, $i(\sigma\tau) = i(\sigma) + i(\tau)$, per tant tenim un homomorfisme de grups injectiu $G \to \mathbb{Z}/n\mathbb{Z}$ i G és un grup cíclic d'ordre divisor de n, diguem $d = |G|$. L'ordre d'un $\sigma \in G$ és l'ordre de $i(\sigma)$ a $\mathbb{Z}/n\mathbb{Z}$. Si σ és un generador de G, $i(\sigma)$ té ordre d a $\mathbb{Z}/n\mathbb{Z}$ i $(\alpha^d)^{\sigma} = (\alpha^{\sigma})^d = \zeta_n^{i(\sigma)d}\alpha^d = \alpha^d$, per tant $\alpha^d \in K$. Com que $[K(\alpha) : K] = d$, no hi pot haver cap potència menor de α que ja estigui a K. □

Teorema 8.3. (*Teorema 90 de Hilbert. Forma additiva*). *Sigui E/K cíclica de grau n, $G = \mathrm{Gal}(E/K)$ i $\sigma \in G$ un generador. Un element $\beta \in E$ té traça $\mathrm{Tr}_{E/K}(\beta) = 0$ si, i només si, existeix un element $\alpha \in E$ amb $\beta = \alpha - \alpha^{\sigma}$.*

PROVA: Si $\beta = \alpha - \alpha^{\sigma}$ és clar que $\mathrm{Tr}(\beta) = 0$. Suposem que $\mathrm{Tr}(\beta) = 0$. Sigui $\gamma \in E$ un element de traça no nul·la. Aleshores l'element

$$\alpha = \frac{1}{\mathrm{Tr}(\gamma)}(\beta\gamma^{\sigma} + (\beta + \beta^{\sigma})\gamma^{\sigma^2} + \cdots + (\beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{n-2}})\gamma^{\sigma^{n-1}})$$

compleix la propietat demanada. □

Teorema 8.4. *Sigui K un cos de característica $p > 0$.*

(a) *Si E/K és una extensió cíclica de grau p, $E = K(\alpha)$, amb α arrel d'algun polinomi $X^p - X - a \in K[X]$.*

(b) *Sigui $a \in K$, α una arrel de $X^p - X - a$ a un cos de descomposició. L'extensió $K(\alpha)/K$ és trivial o cíclica de grau p.*

PROVA: (a) Sigui σ un generador de $G = \mathrm{Gal}(E/K)$. Com que $\mathrm{Tr}(-1) = 0$, pel Teorema 90 de Hilbert (forma additiva) existeix un element $\alpha \in E$ tal que $1 = \alpha - \alpha^\sigma$ Aleshores, per cada $i = 1, \ldots, p$ els elements $\alpha^{\sigma^i} = \alpha + i$ són tots diferents, per tant, α té p conjugats diferents sobre K, per tant té grau p sobre K i $E = K(\alpha)$. A més, $(\alpha^p - \alpha)^\sigma = (\alpha^\sigma)^p - \alpha^\sigma = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$, de manera que $\alpha^p - \alpha$ és fix per G i per tant pertany a K.

(b) Per $i = 0, \ldots, p-1$, $\alpha + i \in K(\alpha)$ són arrels diferents de $X^p - X - a$, per tant, $K(\alpha)$ és un cos de descomposició d'aquest polinomi, clarament separable sobre K. Sigui $G = \mathrm{Gal}(K(\alpha)/K)$. Els elements de G queden completament determinats per la imatge de α. Per cada $\sigma \in G$ existeix un enter $i = i(\sigma)$, determinat només mòdul p, tal que $\alpha^\sigma = \alpha + i(\sigma)$. Clarament, $i(\sigma\tau) = i(\sigma) + i(\tau)$, per tant tenim un homomorfisme de grups injectiu $G \to \mathbb{Z}/p\mathbb{Z}$ i G és un grup cíclic d'ordre dividint p, per tant trivial o d'ordre p. □

9.– Resolució per radicals

Extensions radicals Una extensió *radical* és una extensió R/K obtinguda a partir d'una torre d'extensions simples

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{r-1} \subseteq F_r = R$$

on $F_i = F_{i-1}(\alpha_i)$ per $i = 1 \ldots r$ i α_i és arrel d'un polinomi $X^n - a$ amb $\mathrm{car}\, K \nmid n$ o bé d'un polinomi $X^p - X - a$ amb $p = \mathrm{car}\, K$. Els elements $\alpha_1, \ldots, \alpha_r$ són una *successió de radicals* per l'extensió R/K.

Les extensions radicals són òbviament finites i separables.

Proposició 9.1.

(a) *Siguin $E/F/K$. Si E/F i F/K són radicals, també ho és E/K.*

(b) *L'aixecament i la composició d'extensions radicals són radicals*

(c) *Si E/K és radical també ho és una clausura normal N/K.*

PROVA: (a) Si $\alpha_1, \ldots, \alpha_r$ és una successió de radicals per l'extensió F/K i $\beta_1, \ldots, \beta_s$ és una successió de radicals per l'extensió E/F, aleshores $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ és una successió de radicals per E/K.

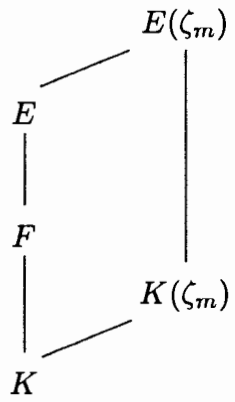
(b) Si $\alpha_1, \ldots, \alpha_r$ és una successió de radicals per l'extensió E/K, també és una successió de radicals per un aixecament EL/L. L'apartat antrerior més el fet que un aixecament d'una radical és radical proven que la composició de radicals és radical.

(c) Com que la composició de les extensions E^σ per totes les K-immersions $\sigma\colon E \to \overline{E}$ és una clausura normal de E/K, aquest apartat és consequència de l'anterior. □

Polinomis resolubles per radicals. Un polinomi separable $f(X) \in K[X]$ és *resoluble per radicals* si existeix alguna extensió radical R/K on f descompon completament. Per l'apartat (c) de la proposició anterior, és equivalent a demanar que existeixi alguna extensió de Galois radical on f descompon completament (ull, pot ser que un cos de descomposició de f no sigui radical pero que ho sigui una extensió més gran).

Teorema 9.2. *Un polinomi separable és resoluble per radicals si, i només si, el grup de Galois d'un cos de descomposició és un grup resoluble.*

PROVA: Suposem que el polinomi $f(X) \in K[X]$ és resoluble per radicals. Sigui E/K una extensió de Galois radical on f descompon completament, i F el cos de descomposició de f dins de E. Sigui $m = [E : K]$ i ζ_m una arrel primitiva m-èsima de la unitat sobre el cos K. Considerem el diagrama



Com que E/K és de Galois radical, l'aixecament $E(\zeta_m)/K(\zeta_m)$ també ho és i té grau dividint m (teorema 7.6-(a) i proposició anterior-(b)). Per tant $E(\zeta_m)$ s'obté com una torre d'extensions simples obtingudes afegint arrels de polinomis $X^n - a$ amb n primer amb la característica de K (i n dividint m) o polinomis $X^p - X - a$ amb $p = \operatorname{car} K$. Per l'apartat (b) dels teoremes 8.2 i 8.4, totes les extensions d'aquesta torre són cícliques de manera que li correspon una torre normal de subgrups de $\mathrm{Gal}(E(\zeta_m)/K(\zeta_m))$ amb quocients cíclics i per tant aquest grup és resoluble. El grup de Galois de l'extensió ciclotòmica $K(\zeta_m)/K$ és abelià i, per tant, també és resoluble. Com que la condició de resoluble es manté per extensió de grups, de la successió exacta

$$1 \longrightarrow \mathrm{Gal}(E(\zeta_m)/K(\zeta_m)) \longrightarrow \mathrm{Gal}(E(\zeta_m)/K) \longrightarrow \mathrm{Gal}(K(\zeta_m)/K) \longrightarrow 1$$

se'n dedueix que $\mathrm{Gal}(E(\zeta_m)/K)$ és resoluble. Com que la condició de resoluble es manté per quocients i $\mathrm{Gal}(F/K)$ és un quocient de $\mathrm{Gal}(E(\zeta_m)/K)$, aquest grup és també resoluble.

Suposem ara que un cos de descomposició de $f(X) \in K[X]$, diguem-li F, té grup de Galois resoluble. Sigui $m = [F : K]$ i ζ_m una arrel primitiva m-èsima de la unitat sobre K. Com que $\mathrm{Gal}(F(\zeta_m)/K(\zeta_m))$ és isomorf a un subgrup de $\mathrm{Gal}(F/K)$, també és resoluble, i el seu ordre divideix m. Per tant, l'extensió $F(\zeta_m)/K(\zeta_m)$ es pot obtenir com una torre d'extensions cícliques que podem suposar de grau primer dividint m. Per l'apartat (a) dels teoremes 8.2 i 8.4, cadascuna d'aquestes extensions és simple generada per un element que és arrel d'un polinomi $X^n - a$ amb n un primer diferent de la característica o d'un polinomi $X^p - X - a$ amb $p = \mathrm{car}\, K$. Per tant $F(\zeta_m)/K(\zeta_m)$ és una extensió radical i com que $K(\zeta_m)/K$ també ho és, $F(\zeta_m)/K$ és una extensió radical on $f(X)$ descompon completament □